valutative periodiche, documentazione relativa a ferie, permessi e malattie, o tabulati contenenti le registrazioni delle presenze in servizio) (*Provv.* 12 maggio 2004).

Il Garante ha ribadito che il riscontro alle richieste di accesso deve essere completo e deve comprendere tutti i dati relativi all'interessato comunque trattati dal titolare, salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali (art. 10, comma 3, del Codice). Ciò, anche nel caso in cui il conferimento all'interessato di determinate qualifiche e ruoli sia ricavabile da atti societari custoditi in archivi aziendali diversi da quelli contenenti i dati connessi alla gestione del rapporto. L'Autorità, nel caso esaminato, ha rilevato che l'interessato aveva dapprima formulato un'istanza in termini tali da potersi ritenere riferita esclusivamente ai dati conservati nel suo fascicolo personale, mentre una richiesta successiva comprendeva, di fatto, tutti i dati personali che lo riguardavano trattati dall'*ex* datore di lavoro. A fronte di questa seconda richiesta, la società era comunque tenuta a individuare tutti i dati personali del lavoratore, a prescindere dalla circostanza che fossero custoditi nel fascicolo personale del lavoratore stesso (*Nota* 9 agosto 2004).

In risposta ad una richiesta di parere presentata da una società, il Garante ha per altro verso sottolineato che, in linea di principio, non può escludersi la necessità di esibire o consegnare al richiedente copia di interi atti o documenti, o parte di essi, riguardanti anche terzi, purché ciò avvenga nel solo caso in cui i dati relativi al richiedente e ai terzi siano intrecciati al punto da risultare incomprensibili o snaturati nel loro contenuto, se privati di alcuni elementi o scomposti rispetto alla loro originaria collocazione (*Nota* 23 novembre 2004).

In merito all'ammissibilità della richiesta dell'interessato di accedere a dati già in suo possesso, l'Autorità ha ricordato che alla richiesta di accesso ai dati deve essere fornito riscontro anche nell'ipotesi in cui le medesime informazioni, in tutto o in parte, siano state comunicate all'interessato o siano comunque dallo stesso detenute. Ciò, al fine di consentire all'interessato di poterne controllare l'esattezza e di chiederne, se del caso, l'aggiornamento, l'integrazione o la correzione. Si è inoltre fatto presente che il diritto di accesso è a volte esercitato chiedendo legittimamente di conoscere anche origine dei dati, finalità, modalità e logica del trattamento, ovvero gli estremi identificativi del titolare e del responsabile del trattamento, ove nominato, nonché dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati (art. 7, comma 2, lett. *e*), del Codice).

Sempre sul tema dell'accesso ai dati personali relativi a dipendenti (in particolare, dati valutativi o contenuti in note di qualifica, dati relativi ad assenze dal servizio per malattia ed altri dati contenuti nei fascicoli personali), sono state numerose anche le decisioni adottate a seguito di ricorso. Unitamente a tali richieste di accesso è stata talvolta manifestata l'opposizione per motivi legittimi al trattamento dei dati: in particolare, in un caso l'istanza era motivata dall'illecita comunicazione di dati riferiti alla carriera professionale del lavoratore ad altre società, in assenza del consenso informato dell'interessato (*Provv.* 3 giugno 2004).

Al termine del 2004 il Garante ha avviato un ciclo di ispezioni per accertare la posizione di alcune *ex* società di fornitura di lavoro interinale e società di ricerca e selezione del personale in materia di notificazione dei trattamenti di taluni dati personali (cfr. par. 20.3)

11.2. *Rapporto di lavoro in ambito pubblico*

Dati sensibili

Nel settore del pubblico impiego, l'Autorità è stata chiamata ad intervenire in vicende in cui, nelle comunicazioni concernenti l'adozione di provvedimenti di gestione interna del personale (trasferimenti o avvicendamenti), sono riportati dati di carattere sensibile riguardanti, in particolare, la salute di dipendenti. Il trattamento di queste informazioni, per perseguire una rilevante finalità d'interesse pubblico di gestione di rapporti di lavoro, può in generale ritenersi lecito. Occorre, tuttavia, che siano rispettati anche i principi di proporzionalità, necessità, pertinenza e non eccedenza dei dati, limitando il trattamento, in ogni sua fase, alle sole informazioni strettamente indispensabili al raggiungimento di tale finalità (artt. 11 e 22 del Codice).

Non è stata così ritenuta rispondente al principio di necessità l'indicazione, nelle comunicazioni indirizzate alle sedi interessate, dei gravi motivi di salute su cui era fondato il provvedimento di trasferimento di un dipendente. Il trasferimento, infatti, avrebbe potuto essere comunicato a tali uffici mediante una nota contenente, in sintesi, il testo del provvedimento originario e gli estremi di riferimento del provvedimento. Tale accorgimento, peraltro, non pregiudica l'obbligo di adeguata motivazione degli atti amministrativi (art. 3, comma 3, l. n. 241/1990), né la facoltà delle persone a ciò legittimate di accedere ad eventuali altri dati, anche di tipo sensibile, contenuti in tali atti, in conformità alle leggi e ai regolamenti in materia di accesso alla documentazione amministrativa.

In materia di trattamento di dati sensibili, l'Autorità ha ritenuto che la disciplina sulla protezione dei dati personali non ponesse ostacoli di fondo ad un'iniziativa del Ministero degli affari esteri consistente nell'identificare i dipendenti portatori di handicap ai fini di esercitazione per evacuazioni antincendio in conformità alla disciplina sull'igiene e la sicurezza del lavoro. Tale attività rientra infatti tra quelle che, sulla base del Codice, possono giustificare il trattamento di dati sensibili (artt. 86, comma 1, lett. *c*) e 112, comma 2, lett. *e*) del Codice).

Nel ricordare, anche in questo caso, che l'amministrazione può effettuare il trattamento delle informazioni relative allo stato di disabilità dei dipendenti soltanto se esse sono realmente *"indispensabili per svolgere attività istituzionali che non possono essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa"* (art. 22, comma 3, del Codice), dovendo altresì rispettare le regole di proporzionalità, indispensabilità, pertinenza e non eccedenza, si è fatto presente al Ministero che, per questa ed altre attività di trattamento di dati sensibili, è necessario provvedere con atto regolamentare ad individuare i tipi di dati che possono essere trattati e le operazioni eseguibili (art. 20, comma 2, del Codice).

Test psico-attitudinali

Con specifico riferimento al trattamento dei dati sensibili nell'ambito della gestione del personale delle forze armate e di polizia, su richiesta della Guardia di finanza, l'Autorità si è espressa in merito all'utilizzo di test psico-attitudinali nelle procedure concorsuali di reclutamento (*Nota* 3 giugno 2004).

Si è precisato, in primo luogo, che il divieto di trattare informazioni sensibili nell'ambito di test psico-attitudinali previsto dal Codice (art. 22, comma 10) si riferisce anche alla raccolta di questi dati mediante questionari volti a costruire il profilo o la personalità dell'interessato. Va pertanto espunta dai questionari utilizzati sia per gli esami psico-attitudinali, sia per quelli psichiatrici, ogni domanda idonea a rivelare profili particolarmente delicati della sfera privata dell'interessato, quali la salute, le abitudini sessuali, le convinzioni politiche, sindacali, religiose, filosofiche o d'altro genere.

A seconda degli esiti di tali esami è invece possibile procedere ad ulteriori accer-

tamenti, ove ritenuto indispensabile, purché questi non consistano nella somministrazione ai candidati di test psico-attitudinali volti a definire il loro profilo o la loro personalità mediante il trattamento di dati sensibili. In questo caso occorre rendere all'interessato una previa e specifica informativa, in modo da consentirgli di non sottoporsi alla prosecuzione della procedura concorsuale e, quindi, a tali ulteriori accertamenti (artt. 13 e 7 del Codice).

Nei ricorsi presentati da alcuni sottufficiali della Guardia di finanza, il Garante ha ritenuto illecita la procedura utilizzata da un comando regionale di stilare un elenco nominativo di tutti i militari in licenza per convalescenza o in aspettativa al fine di regolare l'accesso alla caserma dei dipendenti assenti dal servizio (*Provv.* 7 luglio 2004).

Contrariamente a quanto sostenuto dal comando, l'indicazione del dato relativo all'assenza per "convalescenza" dà luogo ad un trattamento di dati sensibili dal momento che questa informazione, pur non facendo riferimento a specifiche patologie, è comunque suscettibile "di rivelare lo stato di salute del dipendente". Pur non essendo in discussione il potere-dovere della Guardia di finanza di perseguire gli obiettivi di sicurezza della caserma, il trattamento in questione è stato giudicato illecito dal momento che, per disciplinare l'accesso dei militari che si assentano per servizio, non è indispensabile specificare la ragione di tale assenza attinente allo stato di salute, essendo invece sufficiente la sola indicazione dei relativi nominativi.

Nel trattamento di queste informazioni l'amministrazione deve rispettare comunque il principio di indispensabilità, valutando specificamente il rapporto tra i dati sensibili e gli adempimenti legati a compiti e obblighi espletati (artt. 20 e 22 del Codice). Il mancato rispetto di tali garanzie rende il trattamento illecito, anche se effettuato nello svolgimento di funzioni istituzionali o ritenute giustificate da norme di servizio e regolamenti interni.

Visite medico-legali

Non è risultata, invece, contraria alla disciplina sul trattamento dei dati personali la trasmissione alla questura e alla prefettura da parte di un comune (finalizzata all'adozione dei provvedimenti di competenza) dell'esito di alcune visite medico-legali cui era stato sottoposto un dipendente, essendo l'interessato, un agente di pubblica sicurezza, abilitato al porto di pistola, nonché in possesso del porto d'armi per uso di caccia (*Provv.* 22 gennaio 2004). Il caso va visto in connessione con un altro, esaminato da questa Autorità, oggetto di una valutazione parzialmente difforme dell'autorità giudiziaria presso cui è stato impugnato il provvedimento del Garante, in considerazione dell'ulteriore documentazione prodotta dall'interessato, invece non presentata in sede di ricorso all'Autorità (v. par. 19.4). Nel ricorso, il dipendente di una questura aveva lamentato che i dati relativi al proprio stato di salute, accertati nel corso di una visita medica cui era stato sottoposto per verificare la sua idoneità al servizio, erano stati comunicati ad altri soggetti al fine del ritiro cautelativo dell'arma in dotazione e del tesserino di servizio. Nella decisione del ricorso, sulla base degli elementi prodotti dalle parti, il Garante aveva ritenuto che tali comunicazioni fossero avvenute lecitamente, in quanto effettuate in conformità alle norme sulle autorizzazioni di polizia per la detenzione ed il porto d'armi e finalizzate all'adozione dei relativi provvedimenti (*Provv.* 15 gennaio 2004). L'Ufficio, invece, ha avviato specifici accertamenti per verificare se all'interessato sia stata fornita un'idonea informativa anche in relazione ai flussi di dati necessari ai fini dell'adozione dei provvedimenti sull'arma di servizio.

Sempre in materia di trattamento di dati del personale in servizio presso le questure, è stato oggetto di una decisione su ricorso il trattamento di dati sensibili di un funzionario amministrativo. In proposito, il Garante ha segnalato alla questura

la necessità di adottare ogni misura idonea a dare compiuta applicazione alla disciplina relativa agli incaricati del trattamento e a quella concernente le misure minime di sicurezza. Ciò, tenendo anche presente che, in base all'art. 11, comma 2, del Codice, i dati trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati (*Provv.* 7 luglio 2004).

Particolari comunicazioni: in special modo, nell'ambito del procedimento disciplinare

L'utilizzo del fax come mezzo di comunicazione tra amministrazioni è consentito dalla legge e, in linea generale, non è in contrasto con i principi in materia di protezione dei dati personali. Il Garante ha tuttavia evidenziato che per talune circostanze occorre rispettare le specifiche modalità eventualmente previste dalla normativa di settore. Ad esempio, è all'attenzione dell'Autorità una questione relativa alle modalità di trasmissione delle comunicazioni nell'ambito del procedimento disciplinare, per alcune delle quali la normativa prevede la consegna personale all'interessato o, qualora questa non sia possibile, l'invio di una raccomandata (artt. 111 e 104, d.P.R. n. 3/1957). Nel caso in esame, il fax era stato utilizzato anche per le convocazioni dei componenti del Consiglio di disciplina che contenevano il nominativo della persona sottoposta al procedimento, anche se, in ossequio ai principi di pertinenza e non eccedenza, sarebbe stato probabilmente sufficiente anticipare soltanto il tipo di intervento per il quale si richiedeva la presenza del consigliere.

È di nuovo all'esame dell'Autorità la questione dell'indicazione di dati personali dei lavoratori nei buoni pasto (in particolare, i nominativi dei singoli beneficiari e la loro sede di servizio), accanto alle informazioni sul datore di lavoro, nonché dei presupposti di liceità per comunicare i dati dei dipendenti al soggetto tenuto all'erogazione del servizio.

Diritto al lavoro dei disabili

Per quanto riguarda la normativa sul diritto al lavoro dei disabili, è pervenuta una segnalazione con la quale si lamentava che la graduatoria del collocamento obbligatorio, contenente i nominativi di circa tredicimila disabili, era stata pubblicata sul sito *web* del servizio per le politiche del lavoro di una provincia. All'esito degli accertamenti e degli ulteriori approfondimenti effettuati, è stato previsto il blocco del trattamento, visto l'ingente numero di soggetti interessati dalla diffusione indiscriminata di dati idonei a rivelare il loro stato di salute e tenuto conto che le disposizioni di settore (art. 8, legge 12 marzo 1999, n. 68) non definiscono le modalità per garantire la pubblicità degli elenchi e delle graduatorie degli aventi diritto al collocamento obbligatorio.

Anche a tale proposito occorre sottolineare che il divieto di diffusione dei dati idonei a rivelare lo stato di salute è espressamente ribadito dal Codice in relazione allo svolgimento delle attività di concessione di benefici ed agevolazioni previste dalla legge e dai regolamenti.

Un'amministrazione provinciale ha poi informato il Garante, nell'ambito di una comunicazione ai sensi dell'art. 39 del Codice, dell'intenzione di trasmettere ad un comune i dati identificativi degli iscritti ad una lista del collocamento obbligatorio per consentire lo svolgimento di un'indagine sui bisogni dei cittadini disabili. In proposito, l'Autorità ha precisato che, trattandosi di informazioni idonee a rivelare lo stato di disabilità degli interessati, occorre far riferimento alla distinta e più stringente disciplina prevista per il trattamento dei dati sensibili (artt. 20 e 22 del Codice) (*Nota* 21 settembre 2004). Nel corso degli ulteriori approfondimenti, avviati in collaborazione con gli enti pubblici coinvolti, sono state poi fornite indicazioni idonee a realizzare l'iniziativa nel pieno rispetto delle garanzie poste dal Codice a tutela della riservatezza e degli altri diritti dei disabili interessati dall'indagine.

Sciopero nei servizi pubblici essenziali

Con riferimento alla disciplina sullo sciopero nei servizi pubblici essenziali, l'Autorità si è occupata della prassi, seguita da alcune amministrazioni pubbliche, di comunicare al Dipartimento della funzione pubblica della Presidenza del Consiglio dei ministri e all'apposita Commissione di garanzia gli elenchi nominativi di dipendenti che hanno esercitato, in specifici casi, il diritto di sciopero.

In proposito, considerando la chiarezza del dettato normativo della legge n. 146/1990, che pone in capo alle amministrazioni e alle imprese erogatrici di detti servizi l'obbligo di rendere pubblico "il numero dei lavoratori che hanno partecipato allo sciopero, la durata dello stesso e la misura della trattenuta effettuata secondo la disciplina vigente" (art. 5), si è rilevato che talune amministrazioni potevano essere state indotte ad effettuare siffatte comunicazioni da una espressione utilizzata nella circolare del 18 giugno 2002 del Dipartimento della funzione pubblica della Presidenza del Consiglio dei ministri, con riferimento alle rilevazioni delle adesioni allo sciopero.

Per prevenire altri equivoci, l'Ufficio ha pertanto invitato la Presidenza e la Commissione di garanzia a valutare l'opportunità di impartire specifiche istruzioni chiarificatrici sul punto (*Nota* 18 agosto 2004). In proposito, la Commissione ha assicurato al Garante di aver sempre richiesto i soli dati numerici dei lavoratori partecipanti alle astensioni collettive dal lavoro, salvo le ipotesi in cui l'individuazione dell'aderente allo sciopero fosse indispensabile per l'applicazione delle sanzioni previste dalla disciplina di settore.

Concorsi

Il Ministero degli affari esteri ha sottoposto all'attenzione del Garante l'intenzione di consentire ai candidati interessati a partecipare ai concorsi banditi dall'amministrazione di inviare direttamente *on-line* all'ufficio competente la domanda di partecipazione, corredata di dati personali. Poiché la questione attiene alla più generale tematica dell'informatizzazione dell'amministrazione pubblica, il Garante, nelrilevare che l'iniziativa in esame di per sé non era in contrasto con i principi del Codice, ha evidenziato al Ministero che, tuttavia, la disciplina dell'accesso agli impieghi nelle pubbliche amministrazioni e dello svolgimento dei concorsi pubblici (art. 4, d.P.R. n. 487/1994) esclude espressamente l'utilizzo di strumenti diversi dalla diretta presentazione all'ufficio competente delle domande di ammissione al concorso o dal loro invio tramite raccomandata con avviso di ricevimento (*Nota* 25 agosto 2004).

Poiché il trattamento di dati personali da parte di soggetti pubblici è ammesso soltanto per lo svolgimento delle funzioni istituzionali dell'ente, nei limiti stabiliti dalla legge e dai regolamenti, si è quindi indicato all'amministrazione di operare una nuova valutazione dell'iniziativa prospettata, ma in riferimento alla specifica disciplina dei concorsi, piuttosto che rispetto al Codice.

Sempre in tema di trattamento di dati personali nell'ambito di concorsi pubblici, si è precisato che non costituisce violazione della disciplina sulla riservatezza la richiesta, rivolta dalle amministrazioni pubbliche agli aspiranti, di una dichiarazione sostitutiva dei carichi pendenti. Tale procedura tiene conto dell'esigenza dell'amministrazione di verificare l'eventuale presenza di cause ostative all'accesso al pubblico impiego (art. 85, d.P.R. 10 gennaio 1957, n. 3 e art. 2, d.P.R. 9 maggio 1994, n. 487); esigenza quest'ultima espressamente riconosciuta dall'art. 71 del d.P.R. n. 445/2000 e dalla recente riforma del casellario giudiziale, che prevede anche una forma di accesso diretto alla banca dati da parte delle amministrazioni (d.P.R. 14 novembre 2002, n. 313).

11.3. *Previdenza*

Su richiesta di un'associazione di difesa dei diritti dei cittadini, sono all'esame del Garante alcuni moduli adottati dall'Inps con la circolare n. 103 dell'11 maggio 2001, utilizzabili dai lavoratori per presentare le domande di congedo per maternità e di congedo parentale.

In proposito, è necessario valutare alla luce dei principi di indispensabilità, pertinenza e non eccedenza dei dati trattati, la raccolta di informazioni ulteriori rispetto a quelle che, secondo la disciplina sulla tutela delle lavoratrici madri, devono essere necessariamente riportate nel certificato medico di gravidanza (art. 14 d.P.R. 25 novembre 1976, n. 1026).

Maggiori garanzie nelle modalità di raccolta, peraltro, non pregiudicano l'eventuale successiva acquisizione di ulteriori informazioni, anche sensibili, da parte dell'istituto previdenziale o dei medici dei servizi ispettivi del Ministero del lavoro e delle politiche sociali, qualora emerga la reale necessità di svolgere gli accertamenti amministrativi e i controlli previsti (artt. 76 e 77, d.lg. n. 151/2001).

Non è invece in contrasto con i principi di pertinenza e non eccedenza la raccolta, sul modulo di domanda per congedo parentale, dei dati relativi all'altro genitore o affidatario (dati anagrafici, periodi di congedo eventualmente fruiti, tipologia dell'attività lavorativa svolta, ecc.). Tali informazioni sono infatti pertinenti rispetto alla necessità di quantificare il periodo di congedo e la relativa indennità che il datore di lavoro e l'istituto previdenziale devono accordare al genitore richiedente (artt. 32, 33 e 34, d.lg. n. 151/2001) e non risultano eccedenti rispetto alla medesima finalità, non facendo alcun riferimento specifico al tipo di rapporto che intercorre tra i soggetti beneficiari.

L'Autorità, pertanto, è in procinto di definire la questione al fine di invitare l'Inps a riesaminare i moduli per la presentazione delle domande di congedo per maternità, in modo da garantire la riservatezza delle lavoratrici che intendono usufruire dei benefici previsti dalla legge a tutela della maternità.

A seguito di una segnalazione relativa al trattamento dei dati sanitari, l'Autorità si è pronunciata circa le informazioni che devono essere contenute nelle denunce di malattia professionale che i datori di lavoro sono tenuti a trasmettere all'Inail. In tali atti devono essere indicate solo informazioni sanitarie relative o collegate alla patologia denunciata, anziché dati sulla salute inerenti a semplici malesseri accusati o ad assenze registrate nel corso del rapporto di lavoro, non rilevanti per la malattia professionale.

Dati sanitari dei dipendenti

Con un provvedimento del 15 aprile 2004, il Garante ha così vietato all'Inail di utilizzare i dati sanitari di un'assicurata ed ha disposto il blocco di alcune informazioni relative allo stato di salute presenti negli archivi del datore di lavoro e ricavabili dalle diagnosi contenute nei certificati dei lavoratori. All'amministrazione è stato, inoltre, imposto di adottare opportuni accorgimenti per non rendere visibili le diagnosi sulle certificazioni sanitarie detenute.

L'attuale disciplina in materia prevede che il lavoratore assente per malattia sia tenuto a presentare al datore di lavoro solo l'attestazione della prognosi. Può capitare, però, che il certificato contenga un'indicazione non necessaria della diagnosi: in questo caso l'amministrazione non è legittimata a trattare ulteriormente questi dati, e deve adottare opportune misure affinché lavoratori e medici rispettino tali cautele nella redazione dei certificati.

Nel 2004 è stata allo studio dell'Autorità la questione relativa alla trasmissione per via telematica all'Inps dei certificati di malattia predisposti da medici di medi-

cina generale. Al riguardo, il Garante aveva avviato un tavolo di lavoro con i rappresentanti dell'Istituto, al fine di evidenziare gli aspetti relativi alla tutela dei dati personali degli assistiti coinvolti da tale progetto. In particolare, l'Ufficio aveva rappresentato che tale modalità di trasmissione doveva essere prevista da norma di legge o di regolamento essendo difforme da quella prevista dalla disciplina vigente.

Da ultimo, con la legge finanziaria 2005 (art. 1, comma 149, l. n. 311/2004), è stato però stabilito che, a decorrere dal 1° giugno 2005, nei casi di infermità comportante incapacità lavorativa, il medico curante trasmetta all'Inps per via telematica il certificato di diagnosi sull'inizio e sulla durata presunta della malattia. La definizione delle specifiche tecniche e delle modalità procedurali è demandata ad un apposito decreto interministeriale sul quale l'Autorità dovrà fornire il proprio parere ai sensi dell'art. 154, comma 4, del Codice per garantire, in particolare, il rispetto dei principi di pertinenza, non eccedenza e indispensabilità dei dati trattati.

12 Videosorveglianza

12.1. *Protezione dei dati e videosorveglianza*

Nel corso degli ultimi anni si è constatato un forte incremento dell'impiego di sistemi a circuito chiuso, di telecamere e di altri sofisticati strumenti di rilevazione di immagini da parte sia di soggetti pubblici, sia di soggetti privati. Nel corso del 2004 il Garante è ripetutamente intervenuto, intensificando altresì la propria attività ispettiva, a fronte delle sempre più frequenti segnalazioni di cittadini per presunte violazioni della normativa sulla protezione dei dati determinate dall'installazione di impianti di videosorveglianza.

Nel periodo in esame sono stati anche ribaditi i chiarimenti, a più riprese forniti in passato, relativi all'uso privato di telecamere. In particolare, in occasione di un ricorso, l'Autorità ha constatato la mancanza dei presupposti di applicazione del Codice al trattamento dei dati personali effettuato per mezzo di un impianto di videosorveglianza installato da alcuni soggetti presso il cancello di ingresso della propria abitazione (*Provv.* 25 febbraio 2004). Le telecamere così attivate, infatti, configuravano un trattamento effettuato per fini esclusivamente personali. Su questo tipo di trattamenti occorre peraltro verificare quanto richiamato nel citato provvedimento del 29 aprile 2004, sia in relazione alle finalità perseguite, sia in riferimento alla necessità che i dati personali così registrati non siano destinati alla comunicazione sistematica o alla diffusione (in merito v. pure par. 13.1).

Il provvedimento generale sulla videosorveglianza: i principi

Alla luce dell'evoluzione tecnologica, dei nuovi documenti elaborati in sede comunitaria ed internazionale (in particolare, il parere n. 4/2004 dell'11 febbraio 2004 fornito dai Garanti europei, nonché le linee guida espresse dal Consiglio d'Europa il 20-23 maggio 2003) e, soprattutto, delle innovazioni contenute nel Codice, si è reso necessario aggiornare ed integrare il "decalogo" sulla videosorveglianza del novembre 2000, adottando un nuovo provvedimento di carattere generale che stabilisce regole più precise a garanzia dei cittadini (*Provv.* 29 aprile 2004).

Con tale provvedimento sono stati richiamati i principi generali enucleati dal Codice (validi in ambito pubblico e privato) il cui rispetto assicura un equo contemperamento tra le esigenze di sicurezza ed il rispetto della normativa sulla protezione dei dati personali nella rilevazione di immagini e suoni.

Il trattamento deve ovviamente avvenire nel rispetto, oltre che della citata normativa, anche delle prescrizioni contenuti in altre disposizioni di legge che possono interessare l'installazione di apparecchi audiovisivi (come, ad es., in materia di interferenze illecite nella vita privata, tutela della dignità, dell'immagine e del domicilio, tutela dei lavoratori e intercettazioni di comunicazioni e conversazioni).

Con riferimento al principio di necessità, i sistemi di videosorveglianza e il relativi programmi informatici non possono utilizzare dati riferiti a persone identificabili quando le finalità del trattamento possono essere realizzate impiegando solo dati anonimi.

Viene inoltre ribadito che, nel rispetto del principio di proporzionalità, il titolare del trattamento, prima di installare un impianto di videosorveglianza, deve valutare se il suo impiego sia realmente proporzionato agli scopi perseguiti; l'utilizzo di tali

strumenti può essere giustificato, allora, solo quando altre misure (sistemi d'allarme, altri controlli fisici o logistici, misure di protezione agli ingressi ecc.) siano insufficienti o inattuabili.

In applicazione del principio di finalità, il titolare che attiva telecamere deve perseguire scopi determinati, espliciti e legittimi e, non ultimo, di sua pertinenza. È invece emerso che finalità di pubblica sicurezza, prevenzione e accertamento dei reati, pur competendo solo ad organi giudiziari o a forze armate o di polizia, sono state indicate quali finalità perseguite da parte di soggetti pubblici e privati.

Attività dei comuni

È stata ritenuta in contrasto con il principio di finalità l'attivazione da parte di un comune di impianti di videosorveglianza per propaganda turistica, nonché per rendere visibili le condizioni meteorologiche di porti e spiagge. In particolare, l'Autorità ha considerato del tutto ingiustificata l'attività di rilevazione di immagini con finalità promozionali e pubblicitarie, peraltro realizzata attraverso *web cam* dotate di *zoom*, successivamente diffuse sul sito *web* del comune, se in grado di rendere identificabili i cittadini ripresi (*Nota* 15 giugno 2004).

Non sono invece stati rilevati profili di illiceità nell'installazione, da parte di alcuni comuni, di apparecchi in grado di scattare fotografie in prossimità di semafori, al fine di monitorare il traffico e rilevare infrazioni. L'installazione di tali apparecchi che, peraltro, se hanno la finalità di controllare gli accessi ai centri storici, sono disciplinati da un apposito regolamento che ha recepito alcune indicazioni del Garante, non deve essere autorizzata caso per caso dall'Autorità.

Nel recente provvedimento generale sono stati confermati anche gli adempimenti cui sono soggetti tutti i titolari di impianti di videosorveglianza pubblici e privati.

Informativa

I cittadini che si trovano o che transitano in una zona videosorvegliata devono poter essere resi edotti dell'esistenza di sistemi di videosorveglianza, anche attraverso un modello semplificato di informativa "minima", messo a disposizione dal Garante (art. 13, comma 3, del Codice), consistente in un cartello con un simbolo che rappresenta una telecamera, valido per la videosorveglianza posta in essere in aree esterne. In tutte le altre ipotesi, devono essere altresì indicati gli elementi di cui all'art. 13 con particolare riguardo alle finalità e all'eventuale conservazione dei dati.

Prior checking

Nel citato provvedimento generale, il Garante ha anche ricordato che, di regola, l'installazione di sistemi di videosorveglianza non deve essere sottoposta all'esame preventivo dell'Autorità e che non si applica il principio del silenzio-assenso. Pertanto, non può desumersi alcuna approvazione implicita dalla semplice trasmissione al Garante di progetti relativi alla intenzione di installare sistemi di videosorveglianza, peraltro spesso incompleti o comunque privi di quegli elementi che consentirebbero di valutare il rispetto del principio di proporzionalità.

La verifica preventiva da parte dell'Autorità è invece obbligatoria per le tecnologie particolarmente invasive, come quelle che prevedono intrecci, interconnessioni, collegamenti delle immagini con altri particolari dati personali (ad es. biometrici) o in caso di digitalizzazione o indicizzazione delle immagini o di videosorveglianza cd. dinamico-preventiva, che non si limiti a riprendere staticamente un luogo, ma rilevi percorsi, caratteristiche fisionomiche o eventi improvvisi.

Bilanciamento

Per quanto riguarda il settore privato, con il provvedimento in questione ha trovato applicazione anche la disciplina che prevede il bilanciamento di interessi (art. 24, comma 1, lett. *g*), del Codice) individuando i casi in cui è possibile effet-

tuare la rilevazione di immagini anche senza il consenso dell'interessato, ritenendosi prevalente il legittimo interesse del titolare, con un impiego circoscritto dei sistemi di videosorveglianza nei limiti previsti dal provvedimento.

Notificazione

I trattamenti di dati nell'ambito di un'attività di videosorveglianza devono essere notificati al Garante solo se rientrano in una delle ipotesi previste dall'art. 37 del Codice; in ogni caso, non devono essere notificati i trattamenti relativi a comportamenti illeciti o fraudolenti, quando riguardano immagini o suoni conservati temporaneamente per esclusive finalità di sicurezza o di tutela delle persone o del patrimonio (v. *Provv.* 31 marzo 2004, relativo ai casi da sottrarre all'obbligo di notificazione, nonché il *Parere* 23 aprile 2004, recante chiarimenti sui trattamenti da notificare al Garante).

Numerose segnalazioni e reclami sul trattamento di dati effettuato tramite sistemi di videosorveglianza installati da studi professionali, esercizi commerciali, società, enti *no-profit*, hanno reso necessario effettuare accertamenti *in loco* spesso in collaborazione con la Guardia di finanza. In alcuni di questi casi, precedenti all'adozione del nuovo provvedimento generale, è stato necessario contestare gli illeciti di omessa notificazione al Garante del trattamento effettuato mediante impianti di videosorveglianza e/o di mancata adozione di un'idonea informativa agli interessati circa la presenza dei predetti sistemi, comprovata dall'assenza di avvisi o cartelli recanti le indicazioni prescritte dalla vigente normativa in materia di protezione dei dati personali. I relativi titolari del trattamento sono stati, inoltre, richiamati al rispetto delle precise garanzie fissate nel provvedimento del 29 aprile e a fornire un riscontro al riguardo (*Note* 27 ottobre 2004). Anche a seguito dell'adozione del predetto provvedimento del 29 aprile, sono state accertate *in loco* e contestate alcune violazioni dell'obbligo di informativa, che i titolari del trattamento non hanno reso neanche nella forma semplificata suggerita dal Garante con il modulo allegato al provvedimento (v., al riguardo, par. 20.3). In altri casi in cui gli elementi acquisiti in sede ispettiva hanno consentito di escludere la commissione di illeciti da sanzionare, l'Autorità ha comunque richiamato i titolari al rispetto delle prescrizioni contenute nel provvedimento medesimo (*Nota* 29 novembre 2004).

Impianti di videosorveglianza su treni e stazioni

In relazione ad un progetto sperimentale di Trenitalia S.p.A., relativo all'installazione di sistemi di videosorveglianza su taluni vagoni dei treni che transitano su specifiche tratte ferroviarie oggetto di ripetuti atti vandalici e di episodi di microcriminalità a danno dei passeggeri, l'Autorità (v. *Note* 11 novembre 2003 e 25 novembre 2004), preso atto di taluni accorgimenti adottati spontaneamente dalla società a protezione dei dati (effettuazione delle riprese con modalità volte ad escludere l'ingrandimento dell'immagine e la ripresa degli scompartimenti dei passeggeri; memorizzazione delle immagini riprese in forma criptata; predisposizione di un'informativa agli interessati), ha prescritto l'adozione di alcune misure: in particolare, individuare i responsabili e gli incaricati del trattamento; ridurre al minimo, ove tecnicamente possibile, i tempi di conservazione giornaliera delle immagini prima della loro cancellazione; adottare idonee misure di sicurezza dei sistemi e dei dati raccolti. Trenitalia S.p.A. ha recentemente comunicato al Garante che, per ragioni tecnico-organizzative, la sperimentazione non avrebbe avuto inizio prima della fine del 2004, impegnandosi a fornire, entro il primo semestre del 2005, una relazione dettagliata sullo stato di avanzamento del progetto.

Sempre in relazione all'impiego di impianti di videosorveglianza nel settore del trasporto ferroviario, va segnalato un parere che il Garante ha reso ad una società del gruppo Ferrovie dello Stato circa un'iniziativa sperimentale da avviare con la colla-

borazione di una società telefonica (v. *Nota* 29 ottobre 2004). Il progetto consiste nell'installazione presso tre stazioni (Roma Fiumicino, Anzio, Taormina) di alcune telecamere con inquadratura panoramica e rilevazione di immagini a bassa definizione da trasmettere via Internet attraverso il portale *web* della società per finalità di carattere pubblicitario. Gli impianti, inoltre, permettono la visualizzazione delle immagini solo in presa diretta, senza possibilità per l'utente di accedere a registrazioni, né di scaricare le informazioni sul proprio *computer*, o di effettuare variazioni di inquadratura o di dimensioni dell'immagine visualizzata. Il Garante, confermando quanto aveva già precisato con un provvedimento del 14 giugno 2001, ha fatto presente che questo tipo di sistema di videosorveglianza non si pone in contrasto con quanto affermato nel provvedimento del 29 aprile 2004, poiché le telecamere installate non consentono di identificare (neanche indirettamente) gli interessati, in ragione della distanza dal luogo ripreso o delle altre caratteristiche tecniche.

La società ha inoltre sommariamente descritto le caratteristiche di un diverso sistema di videosorveglianza, costituito da telecamere ad alta risoluzione e utilizzato dalla Polizia ferroviaria per finalità di tutela dell'ordine e della sicurezza pubblica. Con lo stesso parere, quindi, l'Autorità ha precisato che quest'ultimo sistema rientra invece nell'ambito applicativo del Codice; e ha altresì sottolineato che il trattamento di dati personali effettuato attraverso l'impianto deve essere pienamente conforme ai principi di necessità, finalità e proporzionalità richiamati nel citato provvedimento generale, e che occorre rispettare, pur in presenza di pericoli concreti o dell'esigenza di prevenzione di specifici reati, le competenze che le leggi assegnano a tali scopi solo ad organi giudiziari e di polizia giudiziaria.

Recentemente l'Autorità ha avuto comunicazione da Trenitalia S.p.A. della messa in servizio, dal 9 settembre 2004, dei treni regionali "Minuetto", dotati di particolari sistemi di videosorveglianza. Si tratta di un'iniziativa scaturita da indicazioni emerse nel corso dei lavoro del Comitato interministeriale sulla sicurezza dei trasporti (Cist) che, ai fini di tutela dell'ordine e sicurezza pubblica, ritiene che tra le misure prioritarie da adottare vi sia anche la videosoveglianza sui treni. L'Autorità è in procinto di definire i termini della propria eventuale attivazione.

12.2. *Videosorveglianza in ambito pubblico*

Frequenti sono stati gli interventi del Garante con riferimento a sistemi di videosorveglianza posti in essere da comuni, da istituti scolastici o da luoghi di cura pubblici.

Ambiti sanitari

A questo riguardo, l'Autorità ha espresso il proprio avviso in ordine alla liceità dell'uso di telecamere presso alcune Asl al fine di assicurare un livello adeguato di sicurezza all'interno dei locali e fronteggiare episodi di aggressione a danno di guardie mediche (*Note* 15 luglio 2004).

L'Autorità ha così precisato che l'eventuale controllo di ambienti sanitari e il monitoraggio di pazienti ricoverati in particolari reparti od ambienti, stante la natura sensibile di alcuni dati che possono essere in tal modo raccolti, devono essere circoscritti ai soli casi di stretta indispensabilità e limitando le riprese a determinati locali e a precise fasce orarie. Deve inoltre essere adottato ogni ulteriore accorgimento necessario per garantire un elevato livello di tutela della riservatezza e della dignità delle persone malate, anche in attuazione delle misure che il Codice prescrive per le strutture sanitarie.

È stato ribadito, inoltre, che il titolare deve assicurare che l'accesso alle immagini sia limitato solo ai soggetti specificamente autorizzati, evitando che siano visionate

da estranei. Rigorose cautele sono state indicate anche in relazione alla possibilità di accedere alle riprese da parte di familiari di ricoverati in reparti dove non sia consentito agli stessi di recarsi personalmente (es. rianimazione). In tali ipotesi, i familiari possono comunque visionare, con gli adeguati accorgimenti tecnici, l'immagine del proprio congiunto. Stante il divieto di divulgazione dei dati idonei a rivelare lo stato di salute, deve essere prevenuto il rischio di diffondere immagini di persone malate su *monitor* accessibili al pubblico.

Esigenze di sicurezza

L'Autorità ha fornito ancora chiarimenti in risposta a quesiti posti da alcuni comandi provinciali dei vigili del fuoco e dall'Istat circa la possibilità di installare sistemi di videosorveglianza presso l'ingresso, l'atrio e il vano scala della sede degli edifici, per ragioni di sicurezza e tutela del patrimonio dell'ente (*Nota* 30 novembre 2004), nonchè per controllare l'accesso del pubblico, onde evitare che utenti esterni possano accedere ad aree vietate (*Note* 15 luglio 2004).

In particolare è stato evidenziato, sulla scorta di precedenti provvedimenti dell'Autorità, che le riprese potrebbero riguardare anche i lavoratori dipendenti e configurare, pertanto, un controllo a distanza nei confronti dei medesimi. A tal proposito, si è richiamata nuovamente 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, con particolare riguardo al principio contenuto nell'art. 4 della l. n. 300/1970 che sancisce il divieto di controllo a distanza dell'attività dei lavoratori.

Istituti scolastici

Con riferimento agli istituti scolastici, è stata sottoposta all'attenzione dell'Autorità la questione riguardante l'installazione di telecamere presso alcuni istituti (*Note* 18 agosto 2004 e 24 dicembre 2004) al fine di controllare gli accessi all'edificio e dissuadere dal compimento di atti di vandalismo.

Al riguardo, è stato evidenziato che l'installazione di sistemi di videosorveglianza può essere giustificata nelle sole aree interessate, soltanto se strettamente indispensabile (ad esempio in caso di ripetuti atti vandalici) e, comunque, al di fuori dell'orario scolastico, quando gli edifici sono chiusi.

È necessario, in ogni caso, rispettare il diritto alla riservatezza dello studente (art. 2, comma 2, d.P.R. n. 249/1998), anche in considerazione del fatto che, frequentemente, lo studente è un minore.

In applicazione di questi principi, l'Autorità è intervenuta a proposito dell'installazione, secondo quanto segnalato da alcune notizie di stampa, di numerose telecamere all'interno e all'esterno di un edificio scolastico. L'Ufficio ha invitato l'istituto a conformarsi alle citate prescrizioni e a produrre ogni documento utile a sostegno delle iniziative assunte (*Nota* 10 settembre 2004), ricevendo un tempestivo riscontro sul quale sono stati però attivati ulteriori accertamenti.

Luoghi di culto

Il Garante è altresì intervenuto al fine di assicurare l'intimità di chi accede a luoghi di culto, quali chiese od altri luoghi di ritrovo dei fedeli, invitando i titolari ad un uso particolarmente prudente dei mezzi di ripresa in ragione del potenziale discriminatorio dei trattamenti riguardanti tali informazioni sensibili, relative alla sfera religiosa dell'individuo, e a limitare l'utilizzo di telecamere nei luoghi di sepoltura ai casi in cui via sia concreto rischio di atti vandalici.

Camere ardenti

Ciononostante, a seguito di un ciclo ispettivo, è stata rilevata l'installazione da parte di un comune di un sistema di videosorveglianza presso un edificio all'interno del quale vengono allestite camere ardenti per la veglia dei defunti. Tali telecamere

non erano segnalate mediante le necessarie informative previste dal Codice, ed anzi erano celate alla vista del pubblico. A seguito di un invito da parte dell'Autorità ad effettuare il blocco spontaneo del trattamento, gli uffici comunali hanno sospeso le attività di videosorveglianza, sulla cui complessiva liceità e sull'eventuale applicazione di sanzioni l'Autorità si esprimerà a breve.

13 Condomìni e multiproprietà

13.1. *Protezione dei dati e condomìni*

Diversi profili di protezione dei dati personali in ambito condominiale, approfonditi negli anni precedenti, sono stati ripresi nel corso del 2004 per rispondere al rilevante numero di segnalazioni e quesiti pervenuti in materia all'Autorità.

In particolare, sono stati posti –sia da parte degli interessati, sia da amministratori di condominio– numerosi quesiti in merito alla diffusione di dati personali riguardanti eventuali situazioni di morosità di singoli condòmini. Ciò, allo scopo di verificare se le modalità di volta in volta utilizzate in concreto, in quanto potenzialmente idonee a rendere tali informazioni accessibili ad un numero indeterminato di soggetti esterni al condominio, fossero compatibili, ed in quali limiti, con le disposizioni contenute nella normativa sulla tutela dei dati personali. Su tale argomento, l'Autorità ha confermato la posizione già assunta in provvedimenti e decisioni adottate nel corso degli anni precedenti.

Il Garante ha avuto modo di precisare che il singolo condòmino può avere conoscenza dei dati disponibili presso l'amministratore, relativi anche agli indirizzi degli altri condòmini, poiché gli indirizzi, così come i nominativi degli interessati, oltre a rendere possibile l'individuazione di ciascun proprietario, sono utili per consentire il regolare svolgimento della vita condominiale (ad esempio, in caso di convocazione dell'assemblea da parte dei condomini o per la comunicazione di avvisi).

L'Autorità ha specificato, inoltre, che i principi in materia di condominio sono applicabili anche nei confronti della gestione di edifici in multiproprietà a scopo residenziale e, con riferimento agli indirizzi di comproprietari che abbiano domicilio o residenza diversi dall'immobile in multiproprietà, qualora ciò sia necessario per particolari e reali esigenze collegate alla gestione della cosa e interessi comuni (*Nota* 11 agosto 2004).

Per contro, in un altro caso sottoposto alla sua attenzione, il Garante ha ribadito che il condominio deve adottare, anche tramite l'amministratore, tutte le cautele necessarie per evitare che terzi non legittimati vengano indebitamente a conoscenza dei dati relativi ai condomini (*Nota* 20 ottobre 2004).

Impianti di videosorveglianza nei condomìni

In relazione al frequente impiego di sistemi di videosorveglianza nei condomìni, il provvedimento del 29 aprile 2004 ha precisato che i videocitofoni sono utilizzabili per identificare coloro che si accingono ad entrare in luoghi privati e che la loro installazione, quando non sono predisposti da persone fisiche per fini esclusivamente personali (art. 5, comma 3, del Codice), deve essere resa nota attraverso un'informativa agevolmente rilevabile.

Quanto all'installazione di vere e proprie telecamere ad iniziativa di singoli condòmini all'interno di edifici in condominio e loro pertinenze (es. posti auto, *box*), il Garante ha precisato che l'impiego di tali sistemi, pur non rientrando nell'ambito di applicazione delle disposizioni del Codice, a meno che i dati siano comunicati sistematicamente o diffusi (art. 5, comma 3, del Codice), richiede comunque l'adozione di cautele a tutela dei terzi. In particolare, l'angolo visuale delle riprese deve essere rigorosamente limitato ai soli spazi di propria esclusiva per-

tinenza, ad esempio antistanti l'accesso alla propria abitazione, escludendo ogni forma di ripresa anche senza registrazione di immagini relative ad aree comuni (cortili, pianerottoli, corridoi, scale, garage comuni) o antistanti l'abitazione di altri condomini; ciò, anche al fine di evitare di incorrere nel reato di interferenze illecite nella vita privata (art. 615-*bis* c.p.).

Il Codice si applica, invece, in caso di installazione di sistemi di ripresa di aree condominiali da parte di più proprietari o condòmini oppure ad iniziativa di un condominio o della relativa amministrazione (comprese le amministrazioni di *residence* o multiproprietà). In questi casi, l'installazione di impianti è ammissibile a condizione che ricorrano determinate finalità, quali l'esigenza di preservare la sicurezza di persone e la tutela di beni in presenza di concrete situazioni di pericolo (di regola costituite da illeciti già verificatisi); la valutazione di proporzionalità, da effettuare anche nei casi di utilizzazione di sistemi di videosorveglianza che non prevedano la registrazione dei dati, va effettuata in rapporto ad altre misure già adottate o che è possibile adottare (es. sistemi comuni di allarme, blindatura o protezione rinforzata di porte e portoni, cancelli automatici).

Un caso particolarmente delicato ha riguardato l'installazione da parte di un condominio di un impianto di videosorveglianza finalizzato a garantire la sicurezza dei condòmini in seguito ad un grave delitto verificatosi in uno stabile vicino. L'Autorità ha ritenuto che, nel caso di specie, trovassero applicazione le prescrizioni e i principi richiamati nel citato provvedimento del 29 aprile, ed ha invitato l'amministrazione del condominio a fornire un riscontro dettagliato su finalità e proporzionalità del trattamento, tempi di conservazione delle immagini registrate, nonché sull'eventuale designazione del responsabile dell'impianto come "responsabile" o "incaricato" del trattamento delle immagini, il quale potrebbe accedere ai dati solo attenendosi alle istruzioni del condominio (*Nota* 5 ottobre 2004).

14 Dati biometrici

14.1. *Protezione dei dati e biometria*

L'impiego di sistemi di rilevazione di impronte digitali comporta chiaramente un trattamento di dati personali, intendendosi in tal senso "*ogni informazione relativa a persona fisica,..., identificat[a] o identificabil[e], anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale*" (art. 4, comma 1, lett. *b*), del Codice). Tale trattamento di dati personali può avvenire solo se proporzionato rispetto alle finalità che si vogliono perseguire: il titolare, prima ancora di dare inizio al trattamento, deve quindi valutare, obiettivamente e con un approccio selettivo, se l'utilizzazione di un sistema di rilevazione delle impronte digitali sia in concreto realmente proporzionata, anche nelle modalità prescelte, rispetto agli scopi prefissi e legittimamente perseguibili.

In questo ambito, sono pervenute all'Ufficio numerose richieste di cittadini relative all'installazione, da parte di alcune banche, di sistemi di rilevazione biometrica per l'accesso alle filiali associati ad apparecchiature di videosorveglianza. In un caso del tutto particolare, originato dalla segnalazione relativa all'utilizzo di un sistema di rilevazione dell'impronta digitale per l'accesso ad una banca, l'Autorità (*Nota* 29 ottobre 2004), ribadendo il chiaro orientamento già espresso che delimita l'uso a casi del tutto eccezionali, valuterà quanto dichiarato dalla banca circa le specifiche e concrete esigenze di sicurezza che hanno giustificato l'installazione dell'impianto (nell'Agenzia segnalata si erano verificati due episodi di rapina). Nel frattempo, ha segnalato interlocutoriamente alla banca la necessità di adottare talune misure: predisporre meccanismi che, in caso di libera indisponibilità dell'utente al rilascio dei propri dati biometrici, gli permettano comunque di accedere alla banca; abbinare il sistema di rilevazione ai comuni dispositivi d'ingresso già in uso, evitando il ricorso a meccanismi complicati ed ulteriori rispetto a quelli già comunemente utilizzati per l'ingresso in banca.

Sul tema dell'impiego da parte delle banche di dati biometrici, eventualmente in associazione a sistemi di videosorveglianza, è in corso un approfondimento con l'Associazione bancaria italiana che, anche a seguito di alcuni incontri con l'Ufficio, si è impegnata a far pervenire gli elementi necessari per consentire all'Autorità di esprimersi nuovamente in materia a seguito di una completa valutazione dell'entità e rilevanza del fenomeno. Uno specifico approfondimento si è avuto, inoltre, in occasione di un convegno organizzato presso la Confindustria.

Il Garante, infine, sta effettuando accertamenti specifici a seguito di alcune segnalazioni circa l'impiego, da parte di talune società, di tecniche di autenticazione biometrica (impronta palmare o facciale) per la rilevazione delle presenze del personale dipendente, in considerazione del fatto che il trattamento di dati biometrici in tale ambito è in molti casi eccedente e ingiustificato alla luce dei principi di necessità e proporzionalità.

Dati biometrici in ambito pubblico

Ulteriori interventi hanno riguardato l'installazione di impianti di rilevazione delle impronte digitali per il controllo degli accessi ai luoghi di lavoro o a servizi di mensa universitaria.

In merito all'iniziativa di un ente regionale per il diritto allo studio, volta ad