15. La videosorveglianza e la biometria

15.1. Videosorveglianza in ambito privato

Verifiche preliminari

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

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

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

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

Vigilanza negli spogliatoi

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

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

volti a evitare riprese indebite di persone negli spogliatoi.

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

Videosorveglianza sui luoghi di lavoro

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

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

La videosorveglianza nei condomini

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

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

Finalità esclusivamente personali

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

ad aree antistanti l'abitazione di altri condomini. Una specifica segnalazione è stata da ultimo inoltrata al Parlamento e al Governo.

15.2. Biometria in ambito pubblico

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

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

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

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

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

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

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

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

Il trattamento dei dati in questione è stato ritenuto dall'Autorità lecito e proporzionato allo scopo. Da una parte, l'attività di identificazione rientrava nelle finalità istituzionali della soprintendenza, la quale, dovendo garantire nel caso di specie elevati standard di sicurezza, aveva necessità di un rigoroso accertamento dell'identità dei dipendenti. Dall'altra, è stato rilevato che le caratteristiche geometriche

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

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

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

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

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

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

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

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

15.3. Videosorveglianza in ambito pubblico

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

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

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

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

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

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

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

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

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

L'Autorità, nuovamente interpellata da alcune amministrazioni in ordine alla necessità di sottoporre taluni trattamenti di dati personali alla verifica preliminare, ha ricordato che il *provvedimento* del 29 aprile 2004 individua espressamente le ipotesi in cui i sistemi di videosorveglianza da attivare devono essere sottoposti alla verifica preliminare del Garante. Spetta, quindi, all'amministrazione richiedente valutare se, nell'ambito di una attività di videosorveglianza, vi siano trattamenti rientranti in quelle ipotesi, da sottoporre all'esame preventivo dell'Autorità.

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

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

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

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

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