Istituto Nazionale
di Previdenza
dell'Amministrazione
Pubblica

Direttore Generale

Roma, 8 LUG. 2010

Ai Dirigenti Generali
Centrali e Regionali

Ai Direttori Regionali

Ai Direttori delle Sedi
Provinciali, Territoriali
e delle Strutture Sociali

Agli Uffici Autonomi di
Trento e Bolzano

Ai Coordinatori delle
Consulenze Professionali

LORO SEDI

All.: n. 2

Circolare n. 15

Oggetto: procedura operativa sulla videosorveglianza.

Premessa

L'Inpdap, al fine di rendere omogenee le procedure adottate dalle strutture dell'Istituto e di favorire la corretta applicazione della normativa sulla protezione dei dati personali (d. lgs. n. 196 del 2003), nel marzo 2010, ha pubblicato la Procedura sulla videosorveglianza, in base alle regole dettate dal Garante per la Protezione dei dati Personali nel "*Provvedimento Generale sulla videosorveglianza" del 29 aprile 2004.*
Successivamente il Garante si è espresso nuovamente in merito, con "*Provvedimento Generale sulla videosorveglianza" dell'8 aprile 2010.*

Tale rivisitazione, benché parziale e volta a recepire le novità di matrice legislativa intervenute, offre l'occasione per precisare alcuni aspetti già affrontati nella Procedura integrandone il contenuto con le nuove istruzioni elaborate dal Garante.
Si invitano, pertanto, tutti i Dirigenti - Responsabili del trattamento dei dati personali, che hanno installato, o, abbiano intenzione di installare, nelle proprie Sedi, apparecchiature di videosorveglianza, ad attuare le indicazioni operative contenute nel seguente documento.

INPDAP
Ufficio Protezione Dati Personali
PROCEDURA OPERATIVA PER LA VIDEOSORVEGLIANZA

1. Scopo e campo di applicazione

Scopo della presente procedura è illustrare le modalità di raccolta, trattamento e conservazione dei dati personali realizzati mediante impianti di videosorveglianza attivati dall'INPDAP.
L'Istituto effettua attività di videosorveglianza ai fini della razionalizzazione e miglioramento dei servizi al pubblico e allo scopo di accrescere la sicurezza degli utenti e del personale. Ulteriore finalità è quella della salvaguardia dei beni patrimoniali ad esso affidati.
Per gli aspetti non direttamente affrontati dalla presente procedura, si rinvia a quanto disposto dal Codice in materia di protezione dei dati personali approvato con decreto legislativo 30 giugno 2003 n. 196 e dal Provvedimento Generale sulla videosorveglianza adottato dal Garante l'8 aprile 2010.

2. Modalità operative.

Alla base dell'installazione di un impianto di videosorveglianza vi è l'attenta valutazione delle esigenze che ne giustificano l'adozione alla luce dei principi di liceità, necessità, proporzionalità e finalità. Prima dell'installazione dell'impianto di videosorveglianza, si dovrà valutare, pertanto, obiettivamente e con un approccio selettivo, se l'utilizzazione ipotizzata sia in concreto realmente proporzionata agli scopi prefissati e legittimamente perseguibili.
Criterio generale è, inoltre, quello della documentazione delle scelte effettuate.
La persistenza dell'esigenza e l'adeguatezza, anche tecnologica, delle diverse opzioni devono essere sottoposte a verifica periodica.

2.1. Analisi preliminare.

A titolo indicativo possono elencarsi le seguenti pre-condizioni:

- verificarsi di episodi che giustificano la scelta: furto, vandalismo, atti di violenza nei riguardi di persone ecc.;
- pericolo concreto del verificarsi di episodi di danno (da valutarsi caso per caso);
- esigenze di tutela di beni patrimoniali economicamente rilevanti (ad es. centri elaborazione dati, strutture di interesse storico-architettonico ecc.);
- esigenze di protezione dell'utenza e dei dipendenti;
- inefficacia di altri accorgimenti per cause connesse alla conformazione della struttura (grandi dimensioni, presenza di numerosi ambienti, autorimesse con angoli nascosti ecc.);
- assenza di altre misure (controlli da parte di addetti, sistemi di allarme, misure di protezione degli ingressi, abilitazione agli ingressi ecc.).

In proposito il Garante per la protezione dei dati personali ha sottolineato che "*non va adottata la scelta semplicemente meno costosa, o meno complicata, o di più rapida attuazione, che potrebbe non tener conto dell'impatto sui diritti degli altri cittadini o di chi abbia diversi interessi legittimi".* In ogni caso non dovranno essere perseguite finalità di sicurezza pubblica (affidate alle competenti autorità), né si dovrà procedere all'installazione di telecamere per meri fini di apparenza o di prestigio.

L'analisi preliminare differisce dalla "verifica preliminare" prevista dal provvedimento dell'8 aprile 2010. Tale ultima attività spetta al Garante qualora vi siano rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità degli interessati, in relazione alla natura dei dati o alle modalità di trattamento o agli effetti che può determinare.

Non ravvisandosi nei sistemi adottati dall'Inpdap – ivi comprese le ipotesi di videosorveglianza integrata con altri enti – casi riconducibili alle fattispecie che necessitano di verifica preliminare, si rinvia al più volte citato provvedimento del Garante per eventuali approfondimenti.

2.2. Fase di progettazione.

Individuate le ragioni che giustificano l'adozione dell'impianto di videosorveglianza, dovranno essere valutate le soluzioni più idonee a realizzare gli obiettivi prefissati alla luce del criterio del minimo impatto sui diritti degli interessati. In questo senso si deve tener conto dei seguenti criteri:

- limitare al minimo la raccolta di immagini dettagliate o l'uso di sistemi che prevedano ingrandimenti evitando riprese inutilmente particolareggiate tali da essere eccessivamente intrusive;
- gli apparecchi non andranno dislocati in aree non soggette a concreti pericoli. Le telecamere dovranno essere installate in modo tale da limitare l'angolo della visuale delle riprese;
- si dovrà procedere alla rilevazione di sole immagini; le telecamere non potranno essere dotate di sistemi di rilevazione sonora che possano configurare l'ipotesi di intercettazione di comunicazioni e conversazioni;
- ove vi siano esigenze di registrazione, il programma informatico di gestione dovrà essere configurato in modo da cancellare o sovrascrivere periodicamente e automaticamente i dati acquisiti;
- occorrerà osservare i limiti di durata della conservazione dei dati nei termini di cui si dirà nei successivi paragrafi.

Il software di gestione deve prevedere sistemi di controllo agli accessi quali user-id e password. Allo stesso modo, devono essere previsti diversi livelli di autorizzazione per accedere alla visione delle immagini registrate (ad es. per manutentore, per responsabile del trattamento, per le forze di polizia).
Nel rispetto dell'art. 4 dello Statuto dei Lavoratori (divieto di controllo a distanza) e del principio di correttezza, le telecamere non devono essere posizionate in modo da rilevare o registrare i lavoratori in aree ricreative (es. mensa, bar, macchine distributrici di alimenti o bibite) o al fine di verificare il rispetto dei doveri di diligenza (es. verifica del rispetto dell'orario di lavoro, orientando la telecamera sul lettore badge). L'inosservanza di tali disposizioni comportano sanzioni penali e amministrative ex artt. 162 co. 2-ter e 171 del Codice Privacy.
Sotto il profilo dell'incidenza sul diritto alla riservatezza di utenti e dipendenti, andrà considerata la possibilità di attivare l'impianto di videosorveglianza nelle sole ore di chiusura della struttura.
Le esigenze che hanno portato all'adozione dell'impianto di videosorveglianza e le relative soluzioni vanno esplicitate in un apposito documento che deve essere conservato e aggiornato periodicamente da parte del Responsabile del trattamento competente.
Assieme al documento debbono essere conservati il progetto preliminare e il progetto definitivo relativi all'impianto comprensivi della dislocazione degli apparecchi video.
La documentazione in argomento dovrà essere presentata alle R.S.U. allo scopo di pervenire all'accordo previsto dall'art. 4 della legge n. 300 del 1970 (Statuto dei Lavoratori).
I medesimi documenti potranno costituire oggetto di mera informativa alle R.S.U. qualora si opti per l'attivazione dell'impianto nelle sole ore di chiusura delle struttura.

2.3. Fase di installazione.

La raccolta dei dati personali rappresentati dalle immagini deve essere necessariamente accompagnata da una chiara informativa che contenga gli elementi previsti dall'art. 13 del "*Codice Privacy*".
Tale informativa viene fornita tramite cartelli da collocarsi nei luoghi ripresi o nelle loro immediate vicinanze, prima del raggio di azione della telecamera (ma non necessariamente a contatto con la stessa). I cartelli, per formato e posizionamento, devono essere chiaramente visibili, anche in orario notturno, inglobando un simbolo o una stilizzazione, che consenta l'immediata comprensione da parte dell'interessato di trovarsi in un'area soggetta a videosorveglianza. I cartelli devono, inoltre, informare esplicitamente e chiaramente gli interessati che le immagini sono rilevate (senza registrazione delle stesse) o registrate.
A tal proposito, il Garante ha previsto un modello di informativa semplificata (modello integrato - allegato 1) che deve rinviare ad un testo completo contenente tutti gli elementi di cui all'art. 13, comma 1, del d. lgs. 196/2003, disponibile senza oneri per l'interessato, con modalità facilmente accessibili, compresi gli strumenti informatici e telematici. L'Istituto ha optato per la pubblicazione nel proprio sito internet del testo completo dell'informativa (Informativa ex art. 13 - allegato 2). Una copia dell'informativa dovrà essere affissa anche nell'albo dell'ufficio o, comunque, in luogo visibile e facilmente accessibile dall'utenza.
Il Garante, inoltre, ha stabilito che l'informativa ex art.13, qualora sia richiesta, deve poter essere resa oralmente da un incaricato. A tal fine, il testo completo dell'informativa dovrà essere messo a disposizione dell'incaricato del servizio reception che la fornirà in caso di richiesta esplicita degli utenti.

Terminate le operazioni di installazione, il fornitore dovrà rilasciare un'apposita dichiarazione che, nel descrivere l'attività effettuata, attesti la conformità dell'impianto alle disposizioni del disciplinare tecnico (regola 25 dell'allegato B al "*Codice Privacy*").

2.4. Gestione dell'impianto e misure di sicurezza.

Il responsabile dovrà provvedere, ai sensi dell'art. 30 del *"Codice Privacy"*, alla designazione per iscritto di tutti gli incaricati indicando espressamente i diversi livelli di autorizzazione al trattamento (visione, conservazione, cancellazione ecc.). Sarà cura del responsabile acquisire l'analogo atto di designazione del soggetto affidatario, in ipotesi di esternalizzazione del servizio.
Sia nel caso di trattamento con incaricati interni sia nell'ipotesi di servizio esternalizzato, si raccomanda di limitare allo stretto necessario il numero degli incaricati autorizzati.
Il Provvedimento dell'8 aprile 2010 elenca idonee e preventive misure di sicurezza per il trattamento dei dati raccolti mediante i sistemi di videosorveglianza, allo scopo di ridurre al minimo i rischi di distruzione, di perdita, anche accidentale, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta.
In particolare il Garante precisa che, in presenza di differenti competenze specificatamente attribuite ai singoli operatori, devono essere configurati diversi livelli di visibilità e trattamento delle immagini.
Inoltre, laddove tecnicamente possibile, in base alle caratteristiche dei sistemi utilizzati, responsabili e incaricati del trattamento, devono essere in possesso di credenziali di autenticazione che permettano di effettuare, a seconda dei compiti attribuiti ad ognuno, unicamente le operazioni di propria competenza.
Qualora i sistemi siano configurati per la registrazione e successiva conservazione delle immagini rilevate, deve essere altresì attentamente limitata la possibilità, per i soggetti abilitati, di visionare non solo in sincronia con la ripresa, ma anche in tempo differito, le immagini registrate e di effettuare sulle medesime operazioni di cancellazione o duplicazione.
Nei casi in cui sia stato scelto un sistema che preveda la conservazione delle immagini, in applicazione del principio di proporzionalità, anche l'eventuale conservazione temporanea dei dati deve essere commisurata al tempo necessario – e predeterminato – a raggiungere la finalità perseguita. La conservazione deve essere limitata a poche ore o, al massimo, alle 24 ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura degli uffici, nonché nel caso in cui si debba aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria.
Il sistema impiegato deve essere programmato in modo da operare, al momento prefissato, l'integrale cancellazione automatica delle informazioni allo scadere del termine previsto da ogni supporto, anche mediante sovra-registrazione, con modalità tali da rendere non riutilizzabili i dati cancellati. In presenza di impianti basati su tecnologia non digitale o comunque non dotati di capacità di elaborazione tali da consentire la realizzazione di meccanismi automatici di *expiring* dei dati registrati, la cancellazione delle immagini dovrà essere effettuata, al termine del periodo prestabilito, sotto il controllo del responsabile. Fino all'espletamento delle operazioni di cancellazione, eventuali supporti di registrazione dovranno essere conservati in contenitori o ambienti ad accesso limitato.
Nel caso di interventi derivanti da esigenze di manutenzione, occorre adottare specifiche cautele; in particolare, i soggetti preposti alle predette operazioni possono accedere alle

immagini solo se ciò si renda indispensabile al fine di effettuare eventuali verifiche tecniche ed in presenza dei soggetti dotati di credenziali di autenticazione abilitanti alla visione delle immagini.
Qualora si utilizzino apparati di ripresa digitali connessi a reti informatiche, gli apparati medesimi devono essere protetti contro i rischi di accesso abusivo di cui all'art. 615-*ter* del codice penale.
La trasmissione tramite una rete pubblica di comunicazioni di immagini riprese da apparati di videosorveglianza deve essere effettuata previa applicazione di tecniche crittografiche che ne garantiscano la riservatezza; le stesse cautele sono richieste per la trasmissione di immagini da punti di ripresa dotati di connessioni wireless (tecnologie *wi-fi, wi-max, Gprs*).

3. Diritti degli interessati.

Secondo l'art. 7 del "*Codice Privacy*" deve essere assicurato agli "interessati identificabili" l'effettivo esercizio dei propri diritti (in particolare quello di accedere ai dati che li riguardano, di verificare le finalità, le modalità e la logica del trattamento e di ottenere l'interruzione di un trattamento illecito, in specie quando non sono adottate idonee misure di sicurezza o il sistema è utilizzato da persone non debitamente autorizzate).
La risposta ad una richiesta di accesso da parte di un "interessato identificabile" a dati conservati deve riguardare esclusivamente quelli attinenti alla sua persona e può comprendere eventuali dati riferiti a terzi solo nei limiti previsti dal "*Codice*" (ovvero nei soli casi in cui la scomposizione dei dati trattati o la privazione di alcuni elementi renda incomprensibili i dati personali relativi all'interessato – v. art. 10, comma 5, del d. lgs. n. 196/2003).
L'identità del richiedente sarà verificata mediante esibizione o allegazione di un documento di identità che evidenzi un'immagine riconoscibile dell'interessato.

IL DIRETTORE GENERALE
Massimo Pianese

Allegato
Modello 1

* In caso di sola rilevazione sostituire “registrazione” con “rilevazione”.

Allegato 2

Istituto Nazionale
di Previdenza
per i Dipendenti
dell'Amministrazione
Pubblica

Ufficio Protezione Dati Personali

Informativa per la videosorveglianza

INFORMATIVA EX ART. 13 D. LGS. 196/2003 IN RELAZIONE AI TRATTAMENTI DI IMMAGINI EFFETTUATI TRAMITE IMPIANTI DI VIDEOSORVEGLIANZA

L'INPDAP, in qualità di "Titolare" del trattamento, ai sensi del d.lgs. 196/2003,

informa

che la raccolta delle immagini tramite impianti di videoregistrazione situati all'ingresso degli edifici dell'Istituto e nelle zone segnalate da appositi cartelli o vetrofanie,

è effettuata

per finalità di razionalizzazione e miglioramento dei servizi resi al pubblico e allo scopo di accrescere la sicurezza degli utenti e del personale. Ulteriore finalità è quella di salvaguardia dei beni patrimoniali dell'Istituto.

I dati raccolti formano oggetto di trattamento nel rispetto del Codice in materia di protezione dei dati personali e della vigente normativa.
I supporti, le immagini e i dati personali in essi contenuti possono essere messi a disposizione esclusivamente nel caso in cui si deve aderire ad una specifica richiesta investigativa dell'Autorità Giudiziaria o di polizia giudiziaria per l'individuazione degli autori di eventuali fatti illeciti a danno dell'Istituto e di altri soggetti.

I dati personali non vengono diffusi.

Il personale dell'Istituto, nonché i soggetti esterni addetti alla gestione e manutenzione delle apposite apparecchiature, hanno accesso ai dati esclusivamente per le sopra citate finalità.
Questi soggetti operano in qualità di "incaricati del trattamento" ai sensi del d.lgs.196/2003.
I supporti contenenti i dati personali vengono conservati in modo da garantire la sicurezza, la riservatezza e la protezione dei dati stessi, nel rispetto delle prescrizioni della normativa vigente, per il solo tempo strettamente necessario al perseguimento delle predette finalità e sono sottoposti alla cancellazione mediante sovra- registrazione non oltre le 24 ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura degli uffici.

Titolare dei dati è l'INPDAP – Istituto Nazionale di Previdenza per i Dipendenti dell'Amministrazione Pubblica, con sede in Roma - Viale A. Ballarin, 42 - presso il quale possono essere esercitati i diritti di cui all'articolo 7 del d.lgs.196/2003.

In particolare l'Interessato ha il diritto di ottenere l'indicazione delle finalità, delle modalità e della logica del trattamento. Inoltre, l'Interessato ha il diritto di ottenere il blocco dei dati trattati in violazione di legge (art. 7 del d. lgs. 196/2003).