Istituto Nazionale Previdenza Sociale

Direzione Centrale Organizzazione

Roma, 09/06/2010

Circolare n. 72

Allegati n. 2

Ai Dirigenti centrali e periferici
Ai Direttori delle Agenzie
Ai Coordinatori generali, centrali e periferici dei Rami professionali
Al Coordinatore generale Medico legale e Dirigenti Medici

e, per conoscenza,

Al Commissario Straordinario
Al Presidente e ai Componenti del Consiglio di Indirizzo e Vigilanza
Al Presidente e ai Componenti del Collegio dei Sindaci
Al Magistrato della Corte dei Conti delegato all'esercizio del controllo
Ai Presidenti dei Comitati amministratori di fondi, gestioni e casse
Al Presidente della Commissione centrale per l'accertamento e la riscossione dei contributi agricoli unificati
Ai Presidenti dei Comitati regionali
Ai Presidenti dei Comitati provinciali

OGGETTO: Provvedimento del Garante per la protezione dei dati personali del 8/4/2010 in materia di videosorveglianza.

SOMMARIO: *Premessa. Provvedimento del Garante privacy del 8/4/2010 in materia di videosorveglianza.*

L'Autorità garante per la protezione dei dati personali, con provvedimento datato 8 aprile 2010, ha disposto nuove regole per l'uso dei sistemi di video sorveglianza.

I dirigenti delle strutture in indirizzo, in qualità di responsabili del trattamento dei dati, avranno cura di dare attuazione alle prescrizioni impartite dall'Autorità, sovrintendendo all'intero processo di trattamento dei dati raccolti attraverso il sistema di videosorveglianza, dalla acquisizione fino all'eventuale cessazione o distruzione, seguendo le istruzioni di cui alla circolare n. 50 del 2007.

1. Posizionamento delle telecamere.

Nel merito, il provvedimento del Garante ribadisce il principio secondo il quale i cittadini che transitano nelle aree sorvegliate devono essere informati, con appositi cartelli, che forniscano gli elementi previsti dall'art. 13 del codice privacy e il cui modello semplificato, allegato al presente messaggio, è peraltro già stato individuato dalla stessa Autorità con provvedimento del 2004.

In relazione ai supporti recanti l'informativa, il Garante ha tuttavia operato alcune precisazioni:
- devono essere collocati prima del raggio d'azione della telecamera, anche nelle sue immediate vicinanze ma non necessariamente a contatto con gli impianti;
- devono avere un formato ed un posizionamento tale da essere visibili in ogni condizione di illuminazione ambientale, anche in orario notturno se il servizio di videosorveglianza è attivo;
- devono informare esplicitamente e chiaramente se le immagini sono soltanto rilevate o anche registrate.
Il numero naturalmente potrà variare in considerazione della vastità dell'area oggetto di rilevamento e delle modalità di riprese.

L'Autorità ritiene auspicabile che l'informativa, resa in forma semplificata, rinvii a un testo completo contenente tutti gli elementi di cui all'art. 13, comma 1, del Codice privacy, disponibile senza oneri per l'interessato, con modalità facilmente accessibili quali strumenti informatici e telematici. Le Sedi potranno pertanto pubblicare l'informativa completa sul sito di riferimento o in apposite bacheche ritenute adatte allo scopo.

I responsabili o un loro incaricato sono tenuti all'occorrenza a fornire, anche oralmente, un'informativa adeguata circa il trattamento dei dati rilevati o registrati.

Nel posizionare le telecamere, il Garante ribadisce il necessario rispetto dell'art. 4 dello Statuto dei lavoratori che vieta i controlli a distanza. Non devono quindi essere effettuate riprese al fine di verificare l'osservanza dei doveri di diligenza, quali il rispetto dell'orario di lavoro o la correttezza nell'esecuzione della prestazione lavorativa (ad es. orientando la telecamera sul *badge*).
Qualora si renda assolutamente necessario, per motivi di sicurezza o esigenze organizzative o produttive, indirizzare la telecamere verso i lavoratori, queste potranno essere istallate soltanto previo accordo con le RSU. In difetto di accordo, su istanza del dirigente responsabile, si seguirà la procedura prevista dallo stesso art. 4 della legge 20 maggio 1970, n. 300 (v., altresì, artt. 113 e 114 del Codice; art. 8 l. n. 300/1970 cit.; art. 2 d.lgs. n. 165/2001).

Si ricorda, che il mancato rispetto di tali disposizioni comporta l'applicazione della sanzione amministrativa stabilita dall'art. 162, comma 2-*ter*, del Codice. Inoltre, l'utilizzo di sistemi di videosorveglianza preordinati al controllo a distanza dei lavoratori o ad effettuare indagini sulle loro opinioni integra la fattispecie di reato prevista dall'art. 171 del Codice.

Sotto un diverso profilo, eventuali riprese televisive sui luoghi di lavoro per documentare attività od operazioni solo per scopi divulgativi o di comunicazione istituzionale o aziendale, e che vedano coinvolto il personale dipendente, possono essere assimilati ai trattamenti temporanei finalizzati alla pubblicazione occasionale di articoli, saggi ed altre manifestazioni del pensiero. In tal caso, alle stesse si applicano le disposizioni sull'attività giornalistica contenute nel Codice (*artt. 136 e ss.*), fermi restando, comunque, i limiti al diritto di cronaca posti a tutela della riservatezza, nonché l'osservanza del codice deontologico per l'attività giornalistica ed il diritto del lavoratore a tutelare la propria immagine opponendosi, per motivi legittimi, alla sua diffusione (*art. 7, comma 4, lett. a), del Codice*).

2. Videosorveglianza integrata con altri Enti.

L'attività di videosorveglianza potrà essere svolta anche in forma integrata con altri Enti tramite la compartecipazione ad un medesimo sistema di rilevazione, al fine di economizzare risorse e mezzi impiegati nell'espletamento delle più diverse attività istituzionali.
In tal caso, l'Autorità ha individuato specifiche prescrizioni:

a) l'utilizzo condiviso, in forma integrale o parziale, di sistemi di videosorveglianza tramite la medesima infrastruttura tecnologica deve essere configurato con modalità tali da permettere ad ogni singolo ente e, in taluni casi, anche alle diverse strutture organizzative dell'ente, l'accesso alle immagini solo nei termini strettamente funzionali allo svolgimento dei propri compiti istituzionali, evitando di tracciare gli spostamenti degli interessati e di ricostruirne il percorso effettuato;

b) nei casi in cui un "centro" unico gestisca l'attività di videosorveglianza per conto di diversi soggetti pubblici, i dati personali raccolti dovranno essere trattati in forma differenziata e rigorosamente distinta, in relazione alle competenze istituzionali della singola pubblica amministrazione.

ll responsabile del trattamento, previa informazione alla Direzione centrale organizzazione, è tenuto a richiedere una verifica preliminare all'Autorità fuori dalle predette ipotesi, ed in tutti i casi in cui i trattamenti effettuati tramite sistemi integrati di videosorveglianza hanno natura e caratteristiche tali per cui le misure e gli accorgimenti sopra individuati non siano integralmente applicabili, in relazione alla natura dei dati o alle modalità del trattamento, agli effetti che possono determinare o, a maggior ragione, con riferimento a quei sistemi per i quali è comunque prevista.

3. Verifiche preliminari

Nel rispetto dell'art. 17 del Codice privacy, l'Autorità garante ribadisce la necessità di chiedere una verifica preliminare allorquando l'attività di videosorveglianza possa comportare dei rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità degli interessati, in relazione alla natura dei dati, alle modalità di trattamento e agli effetti che può determinare.
Nei casi in cui, secondo le prescrizioni del Garante compiutamente descritte al punto 3.2.1 del provvedimento in analisi, debba procedersi ad adire l'Autorità mediante interpello, i responsabili ne daranno preventiva comunicazione alla Direzione Centrale Organizzazione.

4. Misure di sicurezza

I responsabili del trattamento dei dati dovranno verificare l'attività espletata da parte di chi accede alle immagini o controlla i sistemi di ripresa.

Dovranno, altresì, assicurarsi che i dati raccolti siano protetti con idonee e preventive misure di sicurezza, riducendo 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, anche in relazione alla trasmissione delle immagini (artt. 31 e ss. del Codice).

Segnatamente, il provvedimento del Garante stabilisce che le misure di sicurezza dovranno essere rispettose dei seguenti principi:

a) in presenza di differenti competenze specificatamente attribuite ai singoli operatori devono essere configurati diversi livelli di visibilità e trattamento delle immagini. Laddove tecnicamente possibile, in base alle caratteristiche dei sistemi utilizzati, i predetti soggetti, designati incaricati o, eventualmente, responsabili 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;

b) laddove 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;

c) per quanto riguarda il periodo di conservazione delle immagini devono essere predisposte misure tecniche od organizzative per la cancellazione, anche in forma automatica, delle registrazioni, allo scadere del termine previsto;

d) 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;

e) 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;

f) 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*).

5. Conservazione dei dati

Nei casi in cui sia stato scelto un sistema che preveda la conservazione delle immagini, in applicazione del principio di proporzionalità, 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 ventiquattro ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici, nonché nel caso in cui si deve aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria.

Solo in presenza di peculiari esigenze tecniche, può consentirsi la conservazione dei dati per un tempo comunque non superiore alla settimana. La struttura provvederà a manifestare tali eccezionali esigenze alla Direzione Centrale Organizzazione. Allo stesso modo, in tutti i casi in cui si voglia procedere a un allungamento dei tempi di conservazione per un periodo superiore alla settimana, il responsabile dovrà inoltrare richiesta alla Direzione Centrale Organizzazione che provvederà a sottoporla alla prevista verifica preliminare del Garante.

La richiesta, nel rispetto del principio di proporzionalità, dovrà essere adeguatamente motivata con riferimento ad una specifica esigenza di sicurezza perseguita, in relazione a concrete situazioni di rischio riguardanti eventi realmente incombenti e per il periodo di tempo in cui venga confermata tale eccezionale necessità. La congruità del periodo di conservazione può altresì dipendere dalla necessità di aderire ad una specifica richiesta di custodire o consegnare una copia specificamente richiesta dall'autorità giudiziaria o dalla polizia giudiziaria in relazione ad un'attività investigativa in corso.

Il sistema impiegato deve essere programmato in modo da operare al momento prefissato l'integrale cancellazione automatica delle informazioni da ogni supporto allo scadere del termine previsto, 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 eliminazione dei dati registrati, la cancellazione delle immagini dovrà comunque essere effettuata nel più breve tempo possibile.

Il mancato rispetto dei tempi di conservazione delle immagini raccolte e del correlato obbligo di cancellazione di dette immagini oltre il termine previsto comporta l'applicazione della sanzione amministrativa stabilita dall'art. 162, comma 2-*ter*, del Codice.

6. Diritti degli interessati

Si ribadisce il rispetto del Codice privacy, in materia di diritto alla protezione dei dati personali. Pertanto, dovrà 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 (art. 7 del Codice).

La risposta ad una richiesta di accesso a dati conservati deve riguardare tutti quelli attinenti al richiedente identificabile 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 (*art. 10, comma 5, del Codice*).

In riferimento alle immagini registrate non è in concreto esercitabile il diritto di aggiornamento, rettificazione o integrazione in considerazione della natura intrinseca dei dati raccolti, in quanto si tratta di immagini raccolte in tempo reale riguardanti un fatto obiettivo (*art. 7, comma 3, lett. a), del Codice*). Viceversa, l'interessato ha diritto di ottenere il blocco dei dati qualora essi siano trattati in violazione di legge (*art. 7, comma 3, lett. b), del Codice*).

7. Adeguamento.

L'Inps è tenuto ad attenersi a queste nuove prescrizioni, nei termini previsti dallo stesso provvedimento. In caso contrario, il trattamento dei dati risulterà illecito oppure non corretto comportando l'applicazioni di sanzioni.

Per tutto quanto non previsto dal presente massaggio, in particolare per l'ipotesi di servizi si videosorveglianza collegati alle forze di polizia, si rimanda al provvedimento del 8/04/2010, allegato.
Segnatamente, si richiama l'attenzione al modello dei cartelli da posizionare secondo le nuove disposizioni e in cui dovrà sostituirsi il termine "registrazione" a quello di "rilevazione" nel caso in cui le immagini non vengano registrate.

Il Direttore Generale
Nori

Allegato N.1
Allegato N.2