AZIENDA SANITARIA PROVINCIALE DI VIBO VALENTIA

Videosorveglianza Disciplinare aziendale

2010

]

PRIVACY

Premessa 3

1. Trattamento dei dati personali e videosorveglianza: principi generali 3

2. Adempimenti 5

3. Misure di sicurezza 7

4. Settori specifici 10

5. Prescrizioni 12

Premessa

Il Garante per la protezione dei dati personali, con provvedimento emesso in data 8 aprile 2010 e pubblicato sulla G.U. n.99 del 29 aprile 2010, ha emanato le linee guida in materia di videosorveglianza.

Negli anni, infatti, talune disposizioni di legge hanno attribuito ai sindaci e ai comuni specifiche competenze volte a garantire l'incolumità pubblica e la sicurezza urbana (*art. 6, comma 8 d.l. 23 febbraio 2009, n. 11* convertito in legge, con modificazioni, dall'art. 1, comma 1, l. 23 aprile 2009, n. 38; *d.l. 23 maggio 2008, n. 92*, convertito in legge, con modificazioni, dall'art. 1, comma 1, l. 24 luglio 2008, n. 125; il cui art. 6 ha novellato l'*art. 54 del d.lgs. 18 agosto 2000, n. 267*, con cui sono stati disciplinati i compiti del sindaco in materia di ordine e sicurezza pubblica), mentre altre norme, statali e regionali, hanno previsto altresì forme di incentivazione economica a favore delle amministrazioni pubbliche e di soggetti privati al fine di incrementare l'utilizzo della videosorveglianza quale forma di difesa passiva, controllo e deterrenza di fenomeni criminosi e vandalici.

Il provvedimento rappresenta uno strumento particolarmente importante ed utile perché è volto a disciplinare, in assenza di una specifica legislazione in materia, le modalità di utilizzo di immagini raccolte mediante sistemi di videosorveglianza.

Il contenuto del presente Disciplinare è integralmente desunto dalle citate linee guida e la sua puntuale e rigorosa osservanza costituisce un preciso obbligo per i Responsabili e gli Incaricati del trattamento dei dati personali nell'ambito della Azienda Sanitaria Provinciale di Vibo Valentia.

1. Trattamento dei dati personali e videosorveglianza: principi generali

La raccolta, la registrazione, la conservazione e, in generale, l'utilizzo di immagini configura un trattamento di dati personali (*art. 4, comma 1, lett. b), del Codice*). È considerato dato personale, infatti, qualunque informazione relativa a persona fisica identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione.

La Videosorveglianza, nell'ambito dell'Azienda Sanitaria Provinciale di Vibo Valentia, è utilizzata, in generale, per i seguenti fini:

1. *protezione e incolumità degli individui*, ivi ricompresi i profili attinenti alla sicurezza interna ed alla prevenzione dei reati all'interno delle strutture aziendali. E' corretto presumere, infatti, che l'installazione di sistemi di videosorveglianza -e la loro adeguata pubblicizzazione mediante l'informativa- può, in molti casi, svolgere una indubbia funzione di deterrenza;

2. *razionalizzazione e miglioramento dei servizi al pubblico* volti anche ad accrescere la sicurezza degli utenti e degli operatori, nel quadro delle competenze istituzionalmente attribuite all'A.S.P.;

3. *protezione della proprietà aziendale* dagli atti di vandalismo.

L'A.S.P. di Vibo Valentia, al pari di tutti i soggetti pubblici, in qualità di titolare del trattamento (*art. 4, comma 1, lett. f), del Codice*), può trattare dati personali nel rispetto del principio di finalità, perseguendo scopi determinati, espliciti e legittimi (*art. 11, comma 1, lett. b), del Codice*), soltanto per lo svolgimento delle proprie funzioni istituzionali. Ciò vale ovviamente anche in relazione a rilevazioni di immagini mediante sistemi di videosorveglianza (*art. 18, comma 2, del Codice*).

Egualmente, sussiste l'obbligo di fornire previamente l'informativa agli interessati (*art. 13 del Codice*), nei termini fissati dal presente Disciplinare. Pertanto, coloro che accedono o transitano in luoghi dove sono attivi sistemi di videosorveglianza devono essere previamente informati in ordine al trattamento dei dati personali.

Inoltre, la necessità di garantire un livello elevato di tutela dei diritti e delle libertà fondamentali rispetto al trattamento dei dati personali consente l'utilizzo dei sistemi di videosorveglianza solamente ove ciò non determini un'ingerenza ingiustificata nei diritti e nelle libertà fondamentali degli interessati.

Naturalmente l'installazione di sistemi di rilevazione delle immagini deve avvenire nel rispetto, oltre che della disciplina in materia di protezione dei dati personali, anche delle altre disposizioni dell'ordinamento applicabili, quali ad es. le vigenti norme dell'ordinamento civile e penale in materia di interferenze illecite nella vita privata(art. 615 *bis* c.p.), sul controllo a distanza dei lavoratori(legge 20 maggio 1970, n.300) etc..

In tale quadro, pertanto, è necessario che:

a) il trattamento dei dati attraverso sistemi di videosorveglianza sia fondato su uno dei presupposti di liceità che il Codice prevede espressamente per i soggetti pubblici (svolgimento di funzioni istituzionali: *artt. 18-22 del Codice*);

b) ciascun sistema informativo ed il relativo programma informatico vengano conformati già in origine in modo da non utilizzare dati relativi a persone identificabili quando le finalità del trattamento possono essere realizzate impiegando solo dati anonimi (es., configurando il programma informatico in modo da consentire, per monitorare il traffico, solo riprese generali che escludano la possibilità di ingrandire le immagini e rendere identificabili le persone). Lo impone il *principio di necessità*, il quale comporta un obbligo di attenta configurazione di sistemi informativi e di programmi informatici per ridurre al minimo l'utilizzazione di dati personali (*art. 3 del Codice*);

c) l'attività di videosorveglianza venga effettuata nel rispetto del c.d. principio di proporzionalità nella scelta delle modalità di ripresa e dislocazione (es. tramite telecamere fisse o brandeggiabili, dotate o meno di zoom), nonché nelle varie fasi del trattamento che deve comportare, comunque, un trattamento di dati pertinenti e non eccedenti rispetto alle finalità perseguite (*art. 11, comma 1, lett. d) del Codice*).

2. Adempimenti

2.1 Informativa

Gli interessati devono essere sempre informati che stanno per accedere in una zona video sorvegliata.

A tal fine verrà utilizzato il *modello semplificato di informativa "minima"*, indicante il titolare del trattamento e la finalità perseguita, riportato in *fac-simile* nell'allegato n. 1 al presente provvedimento.

In presenza di più telecamere, in relazione alla vastità dell'area oggetto di rilevamento e alle modalità delle riprese, potranno essere installati più cartelli.

Il supporto con l'informativa:

- *deve essere collocato prima del raggio di azione della telecamera*, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti;
- *deve avere un formato ed un posizionamento tale da essere chiaramente visibile* in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno;
- può inglobare un simbolo o una stilizzazione di esplicita e immediata comprensione, eventualmente diversificati al fine di informare se le immagini sono solo visionate o anche registrate.

E' opportuno che l'informativa, resa in forma semplificata avvalendosi del predetto modello, poi rinvii a un testo completo contenente tutti gli elementi di cui all'art. 13, comma 1, del Codice, disponibile agevolmente senza oneri per gli interessati, con modalità facilmente accessibili anche con strumenti informatici e telematici (in particolare, tramite reti Intranet o siti Internet, affissioni in bacheche o locali, avvisi e cartelli agli sportelli per gli utenti).

In ogni caso il Responsabile, anche per il tramite di un Incaricato, ove richiesto è tenuto a fornire anche oralmente un'informativa adeguata, contenente gli elementi individuati dall'art. 13 del Codice.

Le modalità di informativa sopra indicate rappresentano un obbligo per i Responsabili delle stutture aziendali ove sono installati sistemi di videosorveglianza.

2.2 Verifica preliminare

La verifica preliminare viene disciplinata dall'art.17 del Codice.

Al riguardo il Codice stabilisce che *"Le misure e gli accorgimenti di cui al comma 1* (*id est* il trattamento di dati che presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato) *sono prescritti dal Garante in applicazione dei principi sanciti dal codice, nell'ambito di una verifica preliminare all'inizio del trattamento, effettuata anche in relazione a determinate categorie di titolari o di trattamenti, anche a seguito di un interpello del titolare."*.

La verifica preliminare diventa quindi obbligatoria nei casi in cui il trattamento presenti siffatti rischi. Di seguito sono elencati, *esemplificamente*, alcuni casi:

- sistemi di raccolta delle immagini associate a dati biometrici. L'uso generalizzato e incontrollato di tale tipologia di dati può comportare, in considerazione della loro particolare natura, il concreto rischio del verificarsi di un pregiudizio rilevante per l'interessato, per cui si rende necessario prevenire eventuali utilizzi impropri, nonché possibili abusi;

- sistemi di videosorveglianza dotati di *software* che permetta il riconoscimento della persona tramite collegamento o incrocio o confronto delle immagini rilevate (es. morfologia del volto) con altri specifici dati personali, in particolare con dati biometrici, o sulla base del confronto della relativa immagine con una campionatura di soggetti precostituita alla rilevazione medesima;

- sistemi c.d. intelligenti, che non si limitano a riprendere e registrare le immagini, ma sono in grado di rilevare automaticamente comportamenti o eventi anomali, segnalarli, ed eventualmente registrarli. In linea di massima tali sistemi devono considerarsi eccedenti rispetto alla normale attività di videosorveglianza, in quanto possono determinare effetti particolarmente invasivi sulla sfera di autodeterminazione dell'interessato e, conseguentemente, sul suo comportamento. Il relativo utilizzo risulta comunque giustificato solo in casi particolari, tenendo conto delle finalità e del contesto in cui essi sono trattati, da verificare caso per caso sul piano della conformità ai principi di necessità, proporzionalità, finalità e correttezza (*artt. 3 e 11 del Codice*).

- casi in cui si rende necessario, per speciali esigenze di ulteriore conservazione, l'allungamento dei tempi di conservazione dei dati delle immagini registrate oltre il previsto termine massimo di sette giorni, a meno che ciò non derivi da una specifica richiesta dell'autorità giudiziaria o di polizia giudiziaria in relazione a un'attività investigativa in corso.

Anche fuori dalle predette ipotesi, la verifica preliminare è necessaria in tutti i casi in cui i trattamenti effettuati tramite videosorveglianza hanno natura e caratteristiche tali per cui le misure e gli accorgimenti individuati nel presente Disciplinare non siano integralmente applicabili, in relazione alla natura dei dati o alle modalità del trattamento.

La necessità di verifica preliminare deve essere segnalata dal Responsabile al Titolare del trattamento (Direttore Generale) che provvederà ad inoltrarla al Garante.

Il normale esercizio di un impianto di videosorveglianza –al di fuori delle ipotesi sopra elencate- non deve essere sottoposto all'esame preventivo del Garante, sempreché il trattamento medesimo avvenga con modalità conformi al presente Disciplinare.

Nessuna approvazione implicita può desumersi dal semplice inoltro al Garante di documenti relativi a progetti di videosorveglianza cui non segua un esplicito riscontro dell'Autorità, in quanto non si applica il principio del silenzio-assenso

La richiesta di verifica preliminare non deve essere richiesta ove siano rispettate tutte le seguenti condizioni:

a) il Garante si sia già espresso con un provvedimento di verifica preliminare in relazione a determinate categorie di titolari o di trattamenti;

b) la fattispecie concreta, le finalità del trattamento, la tipologia e le modalità d'impiego del sistema che si intende adottare, nonché le categorie dei titolari, corrispondano a quelle del trattamento approvato;

c) si rispettino integralmente le misure e gli accorgimenti conosciuti o concretamente conoscibili prescritti nel provvedimento di cui alla lett. *a*) adottato dal Garante.

2.3 Notificazione

E' regola generale che i trattamenti di dati personali devono essere notificati al Garante solo se rientrano in casi specificamente previsti (*art. 37 del Codice*).

In relazione a quanto stabilito dalla lett. *f*), del comma 1, dell'art. 37, il Garante ha già disposto che non vanno comunque notificati i trattamenti di dati effettuati per esclusive finalità di sicurezza o di tutela delle persone o del patrimonio ancorché relativi a comportamenti illeciti o fraudolenti, quando immagini o suoni raccolti siano conservati temporaneamente (Provvedimento 31 marzo 2004, n. 1/2004, pubblicato in G.U. 6 aprile 2004, n. 81, relativo ai casi da sottrarre all'obbligo di notificazione).

Al di fuori di tali precisazioni, il trattamento, che venga effettuato tramite sistemi di videosorveglianza e che sia riconducibile a quanto disposto dall'art. 37 del Codice, deve essere preventivamente notificato al Garante.

3. Misure di sicurezza

I dati raccolti mediante sistemi di videosorveglianza devono essere 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).

Devono quindi essere adottate specifiche misure tecniche ed organizzative che consentano al titolare di verificare l'attività espletata da parte di chi accede alle immagini o controlla i sistemi di ripresa (se soggetto distinto dal titolare medesimo, nel caso in cui questo sia persona fisica).

E' inevitabile che -in considerazione dell'ampio spettro di utilizzazione di sistemi di videosorveglianza, anche in relazione ai soggetti e alle finalità perseguite nonché della varietà dei sistemi tecnologici utilizzati- le misure minime di sicurezza possano variare anche significativamente. E' tuttavia necessario che le stesse siano quanto meno rispettose dei principi che seguono:

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*).

3.1 Responsabili e incaricati

I Responsabili, formalmente nominati dal Titolare, devono designare per iscritto tutte le persone fisiche, Incaricate del trattamento, autorizzate sia ad accedere ai locali dove sono situate le postazioni di controllo, sia ad utilizzare gli impianti e, nei casi in cui sia indispensabile per gli scopi perseguiti, a visionare le immagini (*art. 30 del Codice*).

Deve trattarsi di un numero delimitato di soggetti, specie quando il titolare si avvale di collaboratori esterni.

Occorre altresì individuare diversi livelli di accesso in corrispondenza delle specifiche mansioni attribuite ad ogni singolo operatore, distinguendo coloro che sono unicamente abilitati a visionare le immagini dai soggetti che possono effettuare, a determinate condizioni, ulteriori operazioni (es. registrare, copiare, cancellare, spostare l'angolo visuale, modificare lo zoom, ecc.).

3.2 Durata dell'eventuale conservazione

Nei casi in cui sia stato scelto un sistema che preveda la conservazione delle immagini, in applicazione del principio di proporzionalità (*v. art. 11, comma 1, lett. e),del Codice*), 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 ventiquattro ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici o esercizi, nonché nel caso in cui si deve aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria.

Solo per peculiari esigenze tecniche può ritenersi ammesso un tempo più ampio di conservazione dei dati che, sulla scorta anche del tempo massimo legislativamente posto per altri trattamenti, non deve comunque superare la settimana.

In tutti i casi in cui si voglia procedere a un allungamento dei tempi di conservazione per un periodo superiore alla settimana, una richiesta in tal senso deve essere sottoposta ad una verifica preliminare del Garante, e comunque essere ipotizzato dal titolare come eccezionale nel rispetto del principio di proporzionalità. La congruità di un termine di tempo più ampio di conservazione va 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 relativa congruità 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 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 comunque essere effettuata nel più breve tempo possibile per l'esecuzione materiale delle operazioni dalla fine del periodo di conservazione fissato dal titolare.

3.3 Diritti degli interessati

Deve essere assicurato agli interessati identificabili l'effettivo esercizio dei propri diritti in conformità al Codice, 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*).

4. Settori specifici

4.1 Rapporti di lavoro

Nelle attività di sorveglianza occorre rispettare il divieto di controllo a distanza dell'attività lavorativa, pertanto è vietata l'installazione di apparecchiature specificatamente preordinate alla predetta finalità: non devono quindi essere effettuate riprese al fine di verificare l'osservanza dei doveri di diligenza stabiliti per il rispetto dell'orario di lavoro e la correttezza nell'esecuzione della prestazione lavorativa (ad es. orientando la telecamera sul *badge*).

Vanno poi osservate le garanzie previste in materia di lavoro quando la videosorveglianza è resa necessaria da esigenze organizzative o produttive, ovvero è richiesta per la sicurezza del lavoro: in tali casi, ai sensi dell'art. 4 della l. n. 300/1970, gli impianti e le apparecchiature, "*dai quali può derivare anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti" (v., altresì, artt. 113 e 114 del Codice; art. 8 l. n. 300/1970 cit.; art. 2 d.lg. n. 165/2001).*

Tali garanzie vanno osservate sia all'interno degli edifici, sia in altri contesti in cui è resa la prestazione di lavoro.

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*).

4.2 Ospedali e strutture sanitarie o luoghi di cura

L'eventuale controllo di ambienti sanitari e il monitoraggio di pazienti ricoverati in particolari reparti o ambienti (ad es. unità di rianimazione, reparti di isolamento), stante la natura sensibile di molti dati che possono essere in tal modo raccolti, devono essere limitati ai casi di comprovata indispensabilità, derivante da specifiche esigenze di cura e tutela della salute degli interessati

Devono essere inoltre adottati tutti gli ulteriori accorgimenti necessari per garantire un elevato livello di tutela della riservatezza e della dignità delle persone malate, anche in attuazione di quanto prescritto dal provvedimento generale del 9 novembre 2005 adottato in attuazione dell'art. 83 del Codice.

Il Responsabile deve garantire che possano accedere alle immagini rilevate per le predette finalità solo i soggetti specificamente autorizzati (es. personale medico ed infermieristico). Particolare attenzione deve essere riservata alle modalità di accesso alle riprese video da parte di terzi legittimati (familiari, parenti, conoscenti) di ricoverati in reparti dove non sia consentito agli stessi di recarsi personalmente (es. rianimazione), ai quali può essere consentita, con gli adeguati accorgimenti tecnici, la visione dell'immagine solo del proprio congiunto o conoscente.

Le immagini idonee a rivelare lo stato di salute non devono essere comunque diffuse (*art. 22, comma 8, del Codice*). In tale quadro, va assolutamente evitato il rischio di diffusione delle immagini di persone malate su *monitor* collocati in locali liberamente accessibili al pubblico.

4.3 Sistemi Integrati di Videosorveglianza

In ottemperanza del principio di economicità delle risorse e dei mezzi impiegati, si è incrementato il ricorso a sistemi integrati di videosorveglianza tra diversi soggetti, pubblici e privati, nonché l'offerta di servizi centralizzati di videosorveglianza remota da parte di fornitori (società di vigilanza, *Internet service providers*, fornitori di servizi video specialistici, ecc.). Inoltre, le immagini riprese vengono talvolta rese disponibili, con varie tecnologie o modalità, alle forze di polizia.

Nell'ambito dei predetti trattamenti, sono individuabili le seguenti tipologie di sistemi integrati di videosorveglianza:

a) *gestione coordinata di funzioni e servizi tramite condivisione, integrale o parziale, delle immagini riprese da parte di diversi e autonomi titolari del trattamento*, i quali utilizzano le medesime infrastrutture tecnologiche; in tale ipotesi, i singoli titolari possono trattare le immagini solo nei termini strettamente funzionali al perseguimento dei propri compiti istituzionali ed alle finalità chiaramente indicate nell'informativa, nel caso dei soggetti pubblici, ovvero alle sole finalità riportate nell'informativa, nel caso dei soggetti privati;

b) *collegamento telematico di diversi titolari del trattamento ad un "centro" unico gestito da un soggetto terzo*; tale soggetto terzo, designato responsabile del trattamento ai sensi dell'art. 29 del Codice da parte di ogni singolo titolare, deve assumere un ruolo di coordinamento e gestione dell'attività di videosorveglianza senza consentire, tuttavia, forme di correlazione delle immagini raccolte per conto di ciascun titolare;

c) sia nelle predette ipotesi, sia nei casi in cui l'attività di videosorveglianza venga effettuata da un solo titolare, si può anche attivare un *collegamento dei sistemi di videosorveglianza con le sale o le centrali operative degli organi di polizia*. L'attivazione del predetto collegamento deve essere reso noto agli interessati. A tal fine deve essere utilizzato il modello semplificato di informativa "minima" - indicante il titolare del trattamento, la finalità perseguita ed il collegamento con le forze di polizia- individuato ai sensi dell'art. 13,

comma 3, del Codice e riportato in *fac-simile* nell'allegato n. 2 al presente Disciplinare. Tale collegamento deve essere altresì reso noto nell'ambito del testo completo di informativa reso eventualmente disponibile agli interessati.

Le modalità di trattamento sopra elencate richiedono l'adozione di specifiche *misure di sicurezza ulteriori*, quali:

1) *adozione di sistemi idonei alla registrazione degli accessi logici degli incaricati e delle operazioni compiute* sulle immagini registrate, compresi i relativi riferimenti temporali, con conservazione per un periodo di tempo congruo all'esercizio dei doveri di verifica periodica dell'operato dei responsabili da parte del titolare, comunque non inferiore a sei mesi;

2) separazione logica delle immagini registrate dai diversi titolari.

Fuori dalle predette ipotesi, 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 o agli effetti che possono determinare, il titolare del trattamento è tenuto a richiedere una verifica preliminare al Garante.

5. Prescrizioni

Le misure necessarie prescritte con il presente Disciplinare devono essere osservate da tutti: Titolare, Responsabili ed Incaricati di trattamento. In caso contrario il trattamento dei dati è, a seconda dei casi, illecito oppure non corretto, ed espone:

- all'inutilizzabilità dei dati personali trattati in violazione della relativa disciplina (*art. 11, comma 2, del Codice*);
- all'adozione di provvedimenti di blocco o di divieto del trattamento disposti dal Garante (*art. 143, comma 1, lett. c*), del Codice), e di analoghe decisioni adottate dall'autorità giudiziaria civile e penale;
- all'applicazione delle pertinenti sanzioni amministrative o penali (*artt. 161 e ss. del Codice*).

Il Direttore Generale
Dott. Luigi Rubens Curia