

***Privacy e Videosorveglianza  
II NUOVO “DECALOGO” 2010***  
(cod.4180)

***Durata:1 ora - Sala:arena HP pad.3 – ore 13:00***

**Massimo Farina**

---

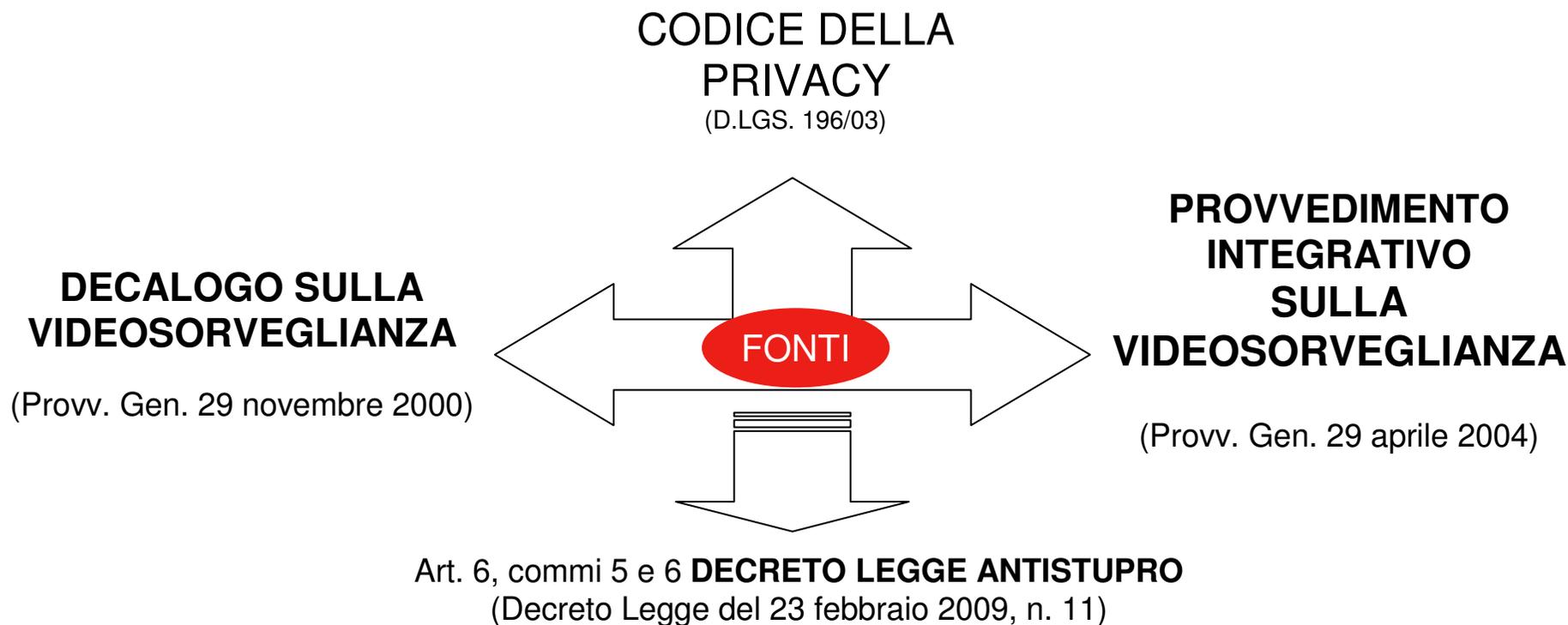
*Docente di  
“Diritto dell'Informatica e delle  
Nuove Tecnologie”  
Università di Cagliari*



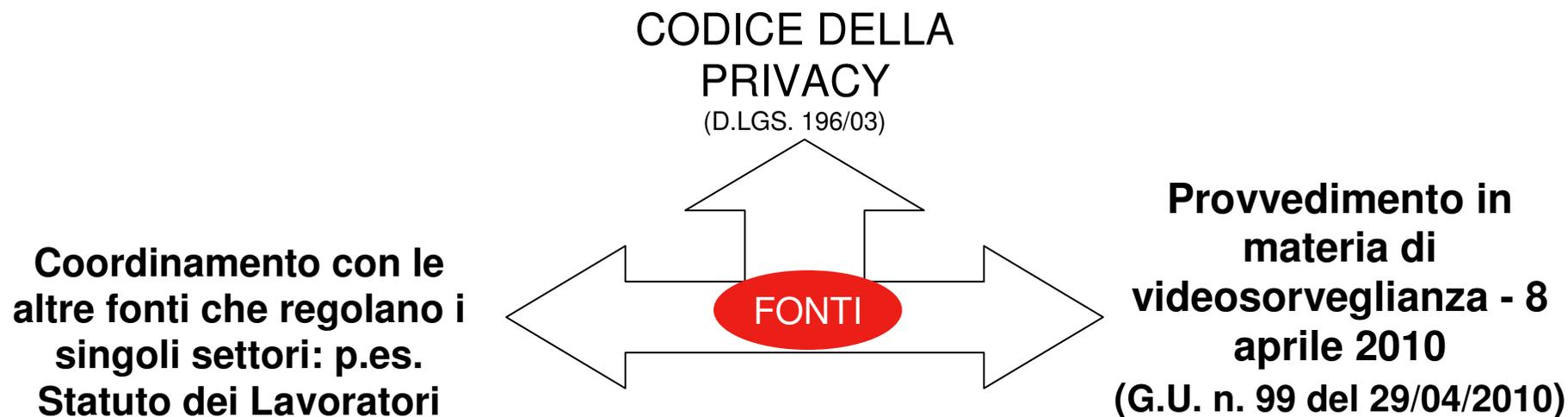
Milano, 20-22 ottobre - Fieramilanocity



UN ANNO FA (SMAU 2009) ..... DOVE CI SIAMO LASCIATI?????



SITUAZIONE ATTUALE (da aprile 2010)



**NOTA:** *“la raccolta, la registrazione, la conservazione e, in generale, l'utilizzo di immagini configura un trattamento di dati personali cioè di informazioni relative a persone fisiche identificate o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione”*

*"è in crescita costante il ricorso alle telecamere di controllo in aree aperte al pubblico e in aree private così come l'utilizzo di tecnologie sofisticate e sistemi miniaturizzati"*



*"In continuo aumento anche l'impiego di dispositivi miniaturizzati o camuffati"*



*"In continuo aumento anche l'impiego di dispositivi miniaturizzati o camuffati"*



**PERSISTONO  
LE CRITICITÀ  
GIÀ  
EVIDENZIATE  
UN ANNO FA**

Assenza di informativa – art. 13 Codice Privacy  
**(informativa semplificata)**



Assenza di adozione di  
idonee misure di sicurezza

Assenza di un regolamento  
interno per il trattamento dei dati

**ESEMPI DI INFORMATIVE INIDONEE**

*"Questo esercizio è servito da un sistema telesorveglianza"*

*"Attenzione: locali muniti di sistema di videosorveglianza"*

*"In questo edificio sono attive telecamere di controllo"*

**Esempio:** trasmissione di dati ripresi dalle telecamere per via telematica (Internet) non protetti da efficaci sistemi di codifica

**Esempi:** Assenza di regole per il trattamento (tempi di registrazione e di archiviazione);  
- Mancata individuazione del responsabile del trattamento e degli incaricati al trattamento;  
- Assenza di regolamentazione per i casi di trattamento in outsourcing (istituti di vigilanza privati).

## PRINCIPIO DI FINALITÀ



chi installa telecamere deve perseguire finalità determinate e di propria pertinenza.

## ESEMPI DI FINALITÀ

- 1) la sicurezza urbana, l'ordine e la sicurezza pubblica, la prevenzione, l'accertamento o la repressione dei reati;
- 2) la protezione della proprietà;
- 3) la rilevazione, prevenzione e controllo delle infrazioni da parte dei soggetti pubblici a ciò preposti dalla legge;
- 4) l'acquisizione di prove.

## IERI

*"Alcune amministrazioni comunali indicano indebitamente, come scopo della sorveglianza, finalità di sicurezza pubblica, prevenzione e accertamento dei reati che competono invece solo ad organi giudiziari o a forze armate o di polizia"*

## OGGI

*"Recenti disposizioni legislative in materia di sicurezza (Decreto Legge antistupro del 23 febbraio 2009) hanno attribuito ai sindaci il compito di sovrintendere alla vigilanza ed all'adozione di atti che sono loro attribuiti dalla legge e dai regolamenti in materia di ordine e sicurezza pubblica, nonché allo svolgimento delle funzioni affidati ad essi dalla legge in materia di sicurezza e di polizia giudiziaria"*

## PRINCIPIO DI LICEITÀ



l'attività di videosorveglianza deve essere conforme alle disposizioni dettate dal d.lgs. 196/03 per ciascuna categoria di titolari (pubblici o privati).

## PRINCIPIO DI NECESSITÀ



Si possono riprendere persone identificabili solo se, per raggiungere gli scopi prefissati, non siano utilizzabili esclusivamente dati anonimi: ad esempio, nel caso di monitoraggio sul traffico, sono consentite soltanto riprese generali, che escludano la possibilità di rendere identificabili le persone.

**PRINCIPIO DI  
PERTINENZA E NON ECCEDENZIA**



**trattamento pertinente e non eccedente, rispetto alle finalità perseguite; ciò si concretizza, ad esempio, nella scelta delle modalità di ripresa e dislocazione delle telecamere (fisse o brandeggiabili, dotate o meno di zoom).**

**NOVITÀ**

***4.5. Utilizzo di web cam o camera-on-line a scopi promozionali-turistici o pubblicitari***

*Le attività di rilevazione di immagini a fini promozionali-turistici o pubblicitari, attraverso web cam devono avvenire con modalità che rendano non identificabili i soggetti ripresi. Ciò in considerazione delle peculiari modalità del trattamento, dalle quali deriva un concreto rischio del verificarsi di un pregiudizio rilevante per gli interessati: le immagini raccolte tramite tali sistemi, infatti, vengono inserite direttamente sulla rete Internet, consentendo a chiunque navighi sul web di visualizzare in tempo reale i soggetti ripresi e di utilizzare le medesime immagini anche per scopi diversi dalle predette finalità promozionali-turistiche o pubblicitarie perseguite dal titolare del trattamento.*

## INFORMATIVA (semplificata)

**Tutti coloro che transitano nelle aree videocontrollate devono essere opportunamente informati della presenza di telecamere attraverso l'affissione di appositi cartelli chiaramente visibili ed esplicativi degli elementi previsti all'art. 13 del d.lgs. 196/03, anche quando il sistema di videosorveglianza è attivo in ORARIO NOTTURNO.**

- **Il Provvedimento del 2010 introduce una nuova tipologia di informativa, per i soggetti privati che effettuano trattamenti di immagini con sistemi di videosorveglianza collegati con le forze di polizia;**
- **Rimane anche l'informativa già adottata con il Provvedimento del 2004**



Milano 21 ottobre 2010

## POSIZIONAMENTO DELL'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.*



**NOTA: Il Garante ritiene auspicabile che l'informativa, resa in forma semplificata [...] poi rinvii a un testo completo contenente tutti gli elementi di cui all'art. 13, comma 1, del Codice [...]**



Milano 21 ottobre 2010

10

## ESENZIONI DALL'OBBLIGO D'INFORMATIVA

(Art. 3.1.1 - Provv. 8 apr. 2010)

Trattamenti svolti dalle forze di polizia, dagli organi di pubblica sicurezza e da altri soggetti pubblici per finalità di **tutela dell'ordine e della sicurezza pubblica, prevenzione, accertamento o repressione dei reati.**

**NOTA:** L'assenza dell'obbligo non significa divieto; infatti, per i titolari dei predetti trattamenti è espressamente prevista la possibilità di *“rendere nota la rilevazione di immagini tramite impianti di videosorveglianza attraverso forme anche semplificate di informativa, che evidenzino, mediante l'apposizione nella cartellonistica di riferimenti grafici, simboli, diciture, l'utilizzo di tali sistemi per finalità di tutela dell'ordine e della sicurezza pubblica, prevenzione, accertamento o repressione dei reati”*.

**SANZIONE AMMINISTRATIVA da seimila euro a trentaseimila euro**

**TEMPO MASSIMO DI CONSERVAZIONE E REGISTRAZIONE DELLE IMMAGINI: "poche ore o, al massimo, ventiquattro ore successive alla rilevazione"**

**ECCEZIONI**

- PER I COMUNI (sicurezza urbana): conservazione dei dati "ai sette giorni successivi alla rilevazione delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza, fatte salve speciali esigenze di ulteriore conservazione".
- peculiari esigenze tecniche (mezzi di trasporto)
- particolare rischiosità dell'attività svolta dal titolare del trattamento (le banche, per le quali può risultare giustificata l'esigenza di identificare gli autori di un sopralluogo nei giorni precedenti una rapina)

**"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"**

**SANZIONE AMMINISTRATIVA da trentamila euro a centottantamila euro**

## POSIZIONAMENTO DELL'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.*



**NOTA: Il Garante ritiene auspicabile che l'informativa, resa in forma semplificata [...] poi rinvii a un testo completo contenente tutti gli elementi di cui all'art. 13, comma 1, del Codice [...]**



Milano 21 ottobre 2010

13

## LA VERIFICA PRELIMINARE del Garante (Art. 3.2 Provv. 8 apr. 2010)

È necessaria in caso di *“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”*.



**Es. Sistemi “intelligenti”:** dotati di software che permettono l'associazione di immagini a dati biometrici (es. "riconoscimento facciale") o in grado, ad esempio, di riprendere e registrare automaticamente comportamenti o eventi anomali e segnalarli (es. "motion detection")

**NOTA:** *“nessuna approvazione implicita può desumersi dal semplice inoltro al Garante di documenti relativi a progetti di videosorveglianza (spesso generici e non valutabili a distanza) cui non segua un esplicito riscontro dell'Autorità, in quanto non si applica il principio del silenzio-assenso”*.

*La provincia di Verona ha sottoposto ai sensi dell'art. 17 del Codice in materia di protezione dei dati personali, il progetto denominato "scuole sicure" con il fine di "tutelare la sicurezza del patrimonio scolastico e delle aree limitrofe, in modo da ottimizzare i risultati dell'azione di contrasto e di repressione della microcriminalità, di atti vandalici e di bullismo"*

#### ESIGENZE DA TUTELARE

- rilevare e ricostruire atti vandalici e di danneggiamento delle strutture scolastiche di proprietà dell'amministrazione provinciale;
- dissuadere da comportamenti contrari all'ordinamento giuridico o da atti di teppismo;
- tutelare il patrimonio contenuto nei plessi scolastici;
- aumentare il senso di sicurezza percepito;
- responsabilizzare gli studenti.

Art. 17. Trattamento che presenta rischi specifici

1. Il trattamento dei dati diversi da quelli sensibili e giudiziari che presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare, è ammesso nel rispetto di misure ed accorgimenti a garanzia dell'interessato, ove prescritti.

2. Le misure e gli accorgimenti di cui al comma 1 sono prescritti dal Garante in applicazione dei principi sanciti dal presente 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.

## **Caratteristiche tecnico-organizzative del sistema centralizzato**

- posizionamento di n. 6 telecamere (fisse o brandeggiabili) in aree perimetrali esterne all'edificio scolastico dell'Istituto scolastico [...] soggette al pubblico passaggio o non sorvegliate dal personale ATA della scuola
- immagini archiviate automaticamente senza che esse possano essere visualizzate in tempo reale;
- riprese effettuate solo in aree esterne alla scuola;
- non si inquadrano i dettagli dei tratti somatici degli interessati;
- zone oggetto di videosorveglianza segnalate da appositi cartelli (informativa semplificata);
- telecamere in funzione solo in orario in cui le strutture scolastiche non sono presidiate da personale in servizio (indicativamente dalle ore 22,00 alle ore 6,30);
- visualizzazione delle immagini consentita solo su richiesta dell'Autorità giudiziaria al responsabile, agli incaricati del trattamento designati, agli appartenenti alle Forze di polizia;
- conservazione dei files delle immagini per un periodo di 72 ore al termine del quale saranno cancellati mediante sovrascrittura;
- installazione di un software di visualizzazione delle immagini e gestione delle telecamere sul PC posto nell'ufficio di presidenza dell'istituto.
- nel solo caso di segnalazione di furti, atti di vandalismo o di eventi dannosi per il patrimonio pubblico, è prevista la riproduzione delle immagini su supporto magnetico per essere messe a disposizione dell'Autorità di polizia o dell'Autorità giudiziaria.

## **MISURE DI SICUREZZA 1/3**

- 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 (v. punto 3.4);**

## **MISURE DI SICUREZZA 2/3**

***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).***

## MISURE DI SICUREZZA 3/3

### SANZIONI

Il mancato rispetto di quanto previsto nelle lettere da a) ad f) appena viste comporta l'applicazione della sanzione amministrativa **da trentamila euro a centottantamila euro** (art. 162, comma 2-ter, del Codice).

L'omessa adozione delle misure minime di sicurezza comporta l'applicazione della sanzione amministrativa **da diecimila euro a centoventimila euro**, e la sanzione penale dell'**arresto sino a due anni**

## **Diritti degli interessati (Art. 3.5 Provv. 8 apr. 2010)**

- Deve essere assicurato agli interessati identificabili il diritto di accedere ai dati che li riguardano, di verificarne 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 [...] 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).
- 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).

**SETTORI SPECIFICI**  
(articolo 4)

**SISTEMI INTEGRATI DI VIDEOSORVEGLIANZA**  
(new)

**RAPPORTI DI LAVORO**

**OSPEDALI E LUOGHI DI CURA**

**VIDEOSORVEGLIANZA**

**TRASPORTO PUBBLICO e TAXI**  
(new)

**WEBCAM A SCOPO TURISTICO**  
(new)

**ISTITUTI SCOLASTICI**

## RAPPORTI DI LAVORO

LIMITI GIÀ IMPOSTI DALLO STAUTO DEI LAVORATORI (L. 300/1970)

divieto di utilizzo di mezzi di sorveglianza a distanza per finalità di mero controllo



divieto di utilizzo di mezzi di sorveglianza a distanza per finalità di mero controllo

Gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive, ovvero dalla sicurezza del lavoro, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali



divieto assoluto di ripresa negli ambienti non destinati al lavoro, quali spogliatoi, docce, armadietti e luoghi ricreativi



Nell'ipotesi in cui il datore di lavoro intenda promuovere la propria attività imprenditoriale con riprese televisive sui luoghi di lavoro, rimane fermo il diritto del lavoratore di opporsi alle riprese



**Decisione del Garante Privacy del 26 febbraio 2009:** Non è lecito installare telecamere che possano controllare i lavoratori, anche in aree e locali dove si trovino saltuariamente (p. es: Aree di carico e scarico)

Milano 21 ottobre 2010

22

## RAPPORTI DI LAVORO

### **Le regole dettate dal decalogo si osservano anche**

- all'interno degli edifici
- in altri contesti in cui è resa la prestazione di lavoro (ad esempio, nei cantieri edili o con riferimento alle telecamere installate su veicoli adibiti al servizio di linea per il trasporto di persone)
- o su veicoli addetti al servizio di noleggio con conducente e servizio di piazza (taxi) per trasporto di persone (le quali non devono riprendere in modo stabile la postazione di guida, e le cui immagini, raccolte per finalità di sicurezza e di eventuale accertamento di illeciti, non possono essere utilizzate per controlli, anche indiretti, sull'attività lavorativa degli addetti).

### **SANZIONI**

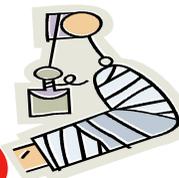
**Il mancato rispetto di quanto sopra prescritto comporta l'applicazione della sanzione amministrativa del pagamento di una somma da trentamila euro a centottantamila euro**

**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 (ammenda da lire 300.000 a lire 3.000.000 o con l'arresto da 15 giorni ad un anno).**

## OSPEDALI E LUOGHI DI CURA (DATI SENSIBILI)



**le riprese devono essere limitate ai casi di stretta indispensabilità**



**Sono autorizzati ad accedere alle immagini solo i soggetti appartenenti al personale medico ed infermieristico**

**Possono, inoltre, accedere alle immagini i familiari di ricoverati in reparti dove non sia consentito agli stessi di recarsi personalmente (per esempio, rianimazione)**

**È FATTO DIVIETO ASSOLUTO DI VISIONE DELLE IMMAGINI AI SOGGETTI ESTRANEI**



**Il mancato rispetto di quanto sopra prescritto comporta l'applicazione della sanzione amministrativa di una somma da trentamila euro a centottantamila euro.**

**La diffusione di immagini in violazione dell'art. 22, comma 8, comporta l'applicazione della sanzione amministrativa da diecimila euro a centoventimila, e della reclusione da uno a tre anni.**

## ISTITUTI SCOLASTICI



Spesso in tali contesti il trattamento riguarderebbe soggetti minori



Le riprese devono essere circoscritte alle sole aree interessate ed attivate negli orari di chiusura degli istituti



### SANZIONI

Il mancato rispetto delle suddette regole comporta l'applicazione della sanzione amministrativa da trentamila euro a centottantamila euro

## Sistemi integrati di videosorveglianza

**collegano telecamere tra soggetti diversi, sia pubblici che privati, o consentono la fornitura di servizi di videosorveglianza "in remoto" da parte di società specializzate (es. società di vigilanza, Internet providers) mediante collegamento telematico ad un unico centro, sono obbligatorie specifiche misure di sicurezza.**

- a) **gestione coordinata di funzioni e servizi** tramite condivisione, delle immagini riprese da parte diversi e autonomi titolari del trattamento, i quali utilizzano le medesime infrastrutture tecnologiche: 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.
- 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

## Sicurezza urbana

**I Comuni che installano telecamere per fini di sicurezza urbana hanno l'obbligo di mettere cartelli che ne segnalino la presenza, salvo che le attività di videosorveglianza siano riconducibili a quelle di tutela specifica della sicurezza pubblica, prevenzione, accertamento o repressione dei reati. La conservazione dei dati non può superare i 7 giorni, fatte salve speciali esigenze.**

**NOTA:** "Non spetta a questa Autorità definire il concetto di sicurezza urbana e delimitarne l'ambito operativo rispetto a quelli di ordine e sicurezza pubblica; purtuttavia, resta inteso che, nelle ipotesi in cui le attività di videosorveglianza siano assimilabili alla tutela della sicurezza pubblica, nonché alla prevenzione, accertamento o repressione dei reati, trova applicazione l'art. 53 del Codice"

## **Violazioni al codice della strada**

obbligatoria i cartelli che segnalino i sistemi elettronici di rilevamento delle infrazioni. Le telecamere devono riprendere solo la targa del veicolo (non quindi conducente, passeggeri, eventuali pedoni). Le fotografie o i video che attestano l'infrazione non devono essere inviati al domicilio dell'intestatario del veicolo.

## **Deposito rifiuti**

Lecito l'utilizzo di telecamere per controllare discariche di sostanze pericolose ed "eco piazzole" per monitorare modalità del loro uso, tipologia dei rifiuti scaricati e orario di deposito.

## ALTRI SETTORI

- **Taxi:** le telecamere non devono riprendere in modo stabile la postazione di guida e la loro presenza deve essere segnalata con appositi contrassegni.
- **Trasporto pubblico:** lecita l'installazione su mezzi di trasporto pubblico e presso le fermate, ma rispettando limiti precisi (es. angolo visuale circoscritto, riprese senza l'uso di zoom).
- **Webcam a scopo turistico:** la ripresa delle immagini deve avvenire con modalità che non rendano identificabili le persone.

*Grazie per l'attenzione*

21 ottobre 2010

***massimo@massimofarina.it***

***http://www.massimofarina.it***

# LICENZA



## Attribuzione - Non Commerciale - Condividi allo stesso modo 2.5

**Tu sei libero di riprodurre, distribuire, comunicare al pubblico, esporre in pubblico, rappresentare, eseguire o recitare l'opera, di creare opere derivate alle seguenti condizioni:**

- **Attribuzione.** Devi riconoscere il contributo dell'autore originario.
  - **Non commerciale.** Non puoi usare quest'opera per scopi commerciali.
  - **Condividi allo stesso modo.** Se alteri, trasformi o sviluppi quest'opera, puoi distribuire l'opera risultante solo per mezzo di una licenza identica a questa.
- 
- **In occasione di ogni atto di riutilizzo o distribuzione, devi chiarire agli altri i termini della licenza di quest'opera.**
  - **Se ottieni il permesso dal titolare del diritto d'autore, è possibile rinunciare ad ognuna di queste condizioni.**
  - **Le tue utilizzazioni libere e gli altri diritti non sono in nessun modo limitati da quanto sopra**