

STAMPA

Videoregistrazione, Videosorveglianza e Privacy

A prima vista, si è portati erroneamente a considerare i Diritti alla Privacy ed alla Sicurezza profondamente inconciliabili tra loro e, poiché uno sembra escludere l'altro, sembra indispensabile sacrificare l'uno a favore dell'altro.

E' nostra opinione che Privacy e Sicurezza debbano entrambi essere considerati Diritti Fondamentali e come tali debbano entrambi essere tutelati. Chi opera eticamente nel nostro settore sente di avere questa importante responsabilità, che può perseguire unicamente nella ricerca della conciliazione tra Privacy e Sicurezza.

Il primo passo, per chi vuole muoversi in questa direzione, consiste nel conseguire un'adeguata conoscenza della materia.

ULTRAK Italia si augura che questa pubblicazione, curata dall'Ing. Claudio Manganelli, uno dei massimi esperti sull'argomento, favorisca la comprensione di quanto disposto dall'Autorità Garante della Privacy e sia quindi di pratico aiuto nella progettazione e realizzazione di sistemi Televisivi a Circuito Chiuso che siano nel contempo efficaci nella protezione e rispettosi della nostra Privacy.

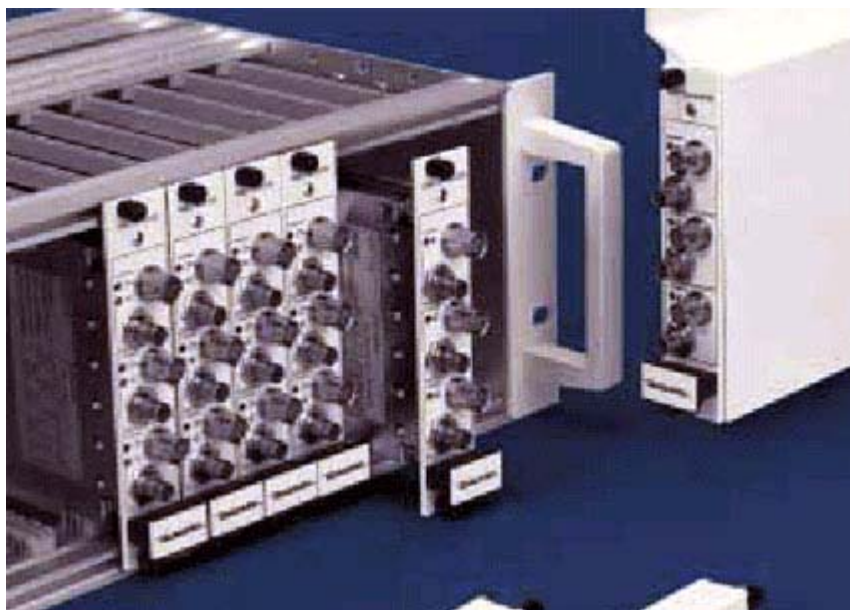


Il Decalogo della Privacy

1. Tutti gli interessati devono determinare esattamente le finalità perseguite attraverso la videosorveglianza e verificarne la liceità in base alle norme vigenti. Se l'attività è svolta in presenza di un pericolo concreto o per la prevenzione di specifici reati, occorre rispettare le competenze che le leggi assegnano per tali fini solo a determinate amministrazioni pubbliche, prevedendo che alla informazioni raccolte possano accedere solo queste amministrazioni.
2. Il trattamento dei dati deve avvenire secondo correttezza e per scopi determinati, espliciti e legittimi (art.9 comma 1, lett. a) e b). legge 675/1996).
3. Nei casi in cui la legge impone la notificazione al Garante dei trattamenti di dati personali effettuati da determinati soggetti (art.7 legge 675/1996), questi devono indicare fra le modalità di trattamento anche la raccolta di informazioni mediante apparecchiature di videosorveglianza.

Non è prevista alcuna altra forma di specifica comunicazione o richiesta di autorizzazione al Garante.

4. Si devono fornire alle persone che possono essere riprese indicazioni chiare, anche se sintetiche, che avvertano della presenza di impianti di videosorveglianza, fornendo anche le informazioni necessarie a sensi dell'art. 10 della legge 675/1996. Ciò è tanto più necessario quando le apparecchiature non siano immediatamente visibili.
5. Occorre rispettare scrupolosamente il divieto di controllo a distanza dei lavoratori e le precise garanzie previste al riguardo (art. 4, legge 300/1970). Lo Statuto dei lavoratori è citato dalla stessa legge 675/art. 43) in modo tale da rendere chiaro il fatto che tale legge resta sempre valida. Pertanto resta fermo il principio di divieto di controllo a distanza dei lavoratori di cui all'art. 4 fermo restando il disposto del comma 2 del medesimo articolo.
6. Occorre rispettare i principi di pertinenza e di non eccedenza, raccogliendo solo i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili e limitando l'angolo visuale delle riprese evitando, quando non indispensabili, immagini dettagliate, ingrandite o dettagli non rilevanti e stabilendo in modo conseguente la localizzazione delle telecamere e le modalità di ripresa.
7. Occorre determinare con precisione il periodo di eventuale conservazione delle immagini, prima delle loro cancellazione e prevedere la loro conservazione solo in relazione ad illeciti o a indagini delle autorità giudiziarie o di polizia.
8. Occorre designare per iscritto i soggetti, responsabili e incaricati del trattamento dei dati (art. 8 e 19 della legge 675/1996) che possono utilizzare gli impianti e prendere visione delle registrazioni, avendo cura che essi accedano ai soli dati personali strettamente necessari e vietando rigorosamente l'accesso ad altri soggetti, salvo che si tratti di indagini giudiziarie o di polizia.
9. I dati raccolti per determinati fini (ad esempio, ragioni di sicurezza, tutela del patrimonio) non possono essere utilizzati per finalità diverse o ulteriori (ad esempio, pubblicità, analisi del comportamenti di consumo), salvo le esigenze di polizia o di giustizia e non possono essere diffusi o comunicati a terzi.
10. I Particolari impianti per la rilevazione degli accessi dei veicoli ai centri storico e alle zone di traffico limitato devono essere conformi anche alle disposizioni contenute nel D.p.R 250/1999. E' altresì fondamentale che la relativa documentazione sia conservata per il solo periodo necessario per contestare le infrazioni e definire il relativo contenzioso e che ad essa si possa inoltre accedere solo a fini di indagine giudiziaria o di polizia.



Tutti gli interessati devono determinare esattamente le finalità perseguite attraverso la videosorveglianza e verificarne la liceità in base alle norme vigenti. Se l'attività è svolta in presenza di un pericolo concreto o per la prevenzione di specifici reati, occorre rispettare le competenze che le leggi assegnano per tali fini solo a determinate amministrazioni pubbliche, prevedendo che alle informazioni raccolte possano accedere solo queste amministrazioni.

Si parla di videosorveglianza o videoregistrazione?

Gli impianti di videosorveglianza, cioè TVCC controllate da monitor senza videoregistrazione, non sono soggetti alla L 675/96 poiché non raccolgono e memorizzano immagini di persone, quindi non trattano dato personali. Le previsioni di leggi, e quindi il decalogo emesso dal Garante, si applicano solamente agli impianti con videoregistrazione. I chiarimenti che seguono, quindi, debbono essere intesi solo per i sistemi con videoregistrazione delle immagini.

Se le riprese sono tali da non consentire il riconoscimento, ma solo il rilevamento dei visitatori, si è comunque soggetti a questi obblighi?

Il decalogo esprime chiaramente la necessità che gli obblighi di legge 675 (notifica, informativa alle persone, protezione dei dati raccolti, trattamento per le sole finalità indicate nell'informativa, conservazione per tempi ragionevolmente contenuti, ecc) siano rispettati quando le immagini sono tali da consentire il riconoscimento delle persone.

Privati e pubblica amministrazione sono sottoposti agli stessi obblighi?

Certamente, a parte gli impianti predisposti ai fini della sicurezza pubblica; persino le installazioni dei varchi di accesso ai centri storici debbono prevedere un'apposita normativa.

Cambia la sostanza se le riprese video sono effettuate entro una proprietà privata non aperta al pubblico? Che obblighi ci sono in questo caso?

Non ci sono obblighi se gli spazi di ripresa non interessano zone comuni ad altre proprietà: casi di questa natura possono avvenire quando, volendo proteggere appartamenti o uffici non aperti al pubblico, le videocamere inquadrano viali o pianerottoli condominiali. In questo caso l'installazione, informandone il condominio, deve essere concordata con le altre proprietà. Se l'accesso agli spazi privati è aperto normalmente a visitatori, si ricade nella previsioni generali.

PUNTO 2

Il trattamento dei dati deve avvenire secondo correttezza e per scopi determinati, espliciti e legittimi (art.9 comma 1, lett. a) e b). legge 675/1996).

Quali sono gli scopi legittimi?

Sono quelli ammessi dall'ordinamento perché non contrastano con norme di legge.

Come faccio a verificare se gli scopi per cui intendo installare l'impianto TVCC sono legittimi?

Il fine per cui pongo in essere il sistema di videosorveglianza non deve essere quello di arrecare danno o disturbo a terzi, ma quello di far valere un mio diritto, come, ad esempio, la difesa dei miei beni. Pertanto, come già sottolineato sopra, dovrò adottare una serie di cautele per l'adozione di tale sistema.

A chi mi rivolgo in caso di dubbi?

Direttamente al Garante (www.garanteprivacy.it).

Devo attendere una risposta? Per quanto tempo vale il principio del "silenzio assenso"?

Il garante ha sicuramente l'obbligo di emanare i propri provvedimenti entro 30 giorni sui ricorsi presentati ai sensi dell'art. 29 legge 675/96. La risposta a quesiti non è invece soggetta a regole, sia

in considerazione dell'elevatissimo numero che ne perviene all'ufficio, sia perché il Garante stesso spesso interviene valutando l'elevato interesse che suscita una determinata problematica e accorpando i vari quesiti con un provvedimento utile a dirimere i relativi dubbi.

PUNTO 3

Nei casi in cui la legge impone la notificazione al Garante dei trattamenti di dati personali effettuati da determinati soggetti (art.7 legge 675/1996), questi devono indicare fra le modalità di trattamento anche la raccolta di informazioni mediante apparecchiature di videosorveglianza. Non è prevista alcuna altra forma di specifica comunicazione o richiesta di autorizzazione al Garante.

Chi deve fare questa notifica?

Il titolare del trattamento è il soggetto tenuto alla notifica (art 7, i. 675).

Che responsabilità si assumono l'installatore e il progettista di fronte al Garante?

Il titolare del trattamento, l'eventuale responsabile del trattamento e l'incaricato del trattamento sono le figure presenti nella 675. Ognuno di loro ha delle responsabilità.

Chi installa non tratta dati personali, ma esegue una fornitura commissionata dal titolare o dal responsabile, questi ultimi soggetti tratteranno i dati e loro sono quindi soggetti al controllo sul corretto operato.

Esiste un modello di riferimento per la notificazione?

L'art. 7 della legge 675 prevede una notifica "una tantum" da parte del titolare per tutti i trattamenti eseguiti (informatici, videosorveglianza, cartacei, ecc). Il modello da compilare è rinvenibile con le spiegazioni sulla compilazione (**vedi box 1**) in vari siti, tra cui quello ufficiale del Garante, o distribuito gratuitamente presso gli uffici postali (**vedi box 2**).

BOX 1

Dal sito www.garanteprivacy.it – FAQ

Per il trattamento dei dati personali è prevista la notificazione al Garante, fermi restando gli obblighi di informativa agli interessati e di acquisizione del consenso. L'art. 7 della L. 675/96 specifica che la notificazione è effettuata preventivamente. Ciò significa che prima di iniziare un trattamento di dati deve essere inviata la notificazione al Garante.

A quale indirizzo va inviata la notificazione?

Il nuovo indirizzo del Garante al quale notificare il trattamento dei dati personali è: **Piazza di Monte Citorio 121, 00186 Roma**. Utilizzando il vecchio indirizzo, comunque la posta arriverebbe al nuovo indirizzo.

Dove sono reperibili i modelli?

I modelli sono reperibili gratuitamente presso tutti gli uffici postali. I modelli sono a disposizione sia in forma cartacea che con floppy disk. A corredo della modulistica vengono distribuiti prestampati: le istruzioni, la busta, la cartolina per la ricevuta di ritorno e il bollettino di c/c postale per il versamento dei diritti di segreteria. La modulistica è altresì reperibile presso al Sezione Modulistica del sito www.garanteprivacy.it.

Che differenza c'è tra la notificazione effettuata con modello cartaceo e quella con floppy disk?

L'utente può effettuare la notificazione indifferentemente su modello cartaceo oppure utilizzando il floppy disk. Cambia solo l'importo dei diritti di segreteria: nel primo caso l'importo è di £.25.000 e nel secondo caso, di £.15.000. Il versamento dei diritti di segreteria va effettuato sul c/c n.97204002 intestato a Garante per la protezione dei dati personali. Se si utilizza il floppy disk, è però indispensabile seguire correttamente le procedure di installazione

del programma sull'hard disk del computer, compilazione delle maschere a video, stampa della notifica, firma, salvataggio del contenuto su un altro disco vergine, controllo che sul dischetto compaia il file notifica.mdb, spedizione del dischetto insieme alla stampa e alla ricevuta di c/c. con raccomandata a/r.

Il dischetto ritirato all'ufficio postale va spedito al Garante?

No. Il dischetto ritirato presso gli uffici postali contiene il programma per effettuare la notificazione. Il programma va riversato sul computer, digitando a:install.exe, in maniera da potere inserire poi i dati nelle maschere che compariranno a video. Una volta inseriti tutti i dati, essi vanno salvati su un altro dischetto vergine. Il salvataggio avviene "cliccando" sulla prima icona in basso a destra dello schermo rappresentante un floppy disk. Tale operazione provoca la scrittura sul dischetto di un file denominato "notifica.mdb" leggibile tra l'altro, anche tramite il database Access della Microsoft. E' questo il floppy da inviare al Garante, unitamente alla stampa del suo contenuto firmata dal titolare e dagli eventuali responsabili. Per stampare il contenuto del floppy contenente la notificazione, basta "cliccare" sulla seconda icona a destra che raffigura la stampante e seguire le istruzioni che compaiono a video (per stampare singoli riquadri o l'intera notificazione).

A chi si versano i diritti di segreteria?

Al "Garante per la protezione dei dati personali", Piazza di Monte Citorio, 121 - 00186 Roma, mediante conto corrente postale n.97204002, Causale: Diritti di segreteria. La ricevuta del versamento va allegata alla notifica, sia nel caso di notificazione su floppy che su modello. Una matrice del c/c va trattenuta da chi ha effettuato il versamento, l'altra va allegata alla notificazione.

Cosa bisogna fare in caso di modifica della precedente notificazione?

La modifica va notificata al Garante utilizzando lo stesso modello usato per la notificazione (indifferentemente floppy disk oppure modello cartaceo) e compilando solo il frontespizio, il quadro a, i quadri interessati alla modifica e il quadro p con la firma del notificante e, nel caso di nuovi responsabili, con la loro firma. Va quindi trasmessa al Garante con raccomandata a/r come per la prima notificazione. Nel caso di modifica presentata su disco, occorre inviare un nuovo disco che contenga tutti i dati della precedente notificazione aggiornati. Non è infatti possibile compilare solo i singoli riquadri modificati. In pratica è necessario utilizzare una copia della precedente notificazione.

In caso di modifica del titolare si deve compilare il riquadro a) con la nuova denominazione. Come si fa a riferire la modifica al 'vecchio titolare'?

Nel caso di modifica inviata con modello cartaceo, si può inviare una lettera di accompagnamento che sia esplicativa, oppure, sempre nel riquadro a) indicare il "vecchio titolare" con la menzione "modificato in", seguito dalla nuova denominazione. Nel caso di modifica trasmessa su floppy disk è necessaria la lettera di accompagnamento.

In caso di cessazione del trattamento, cosa si deve fare?

La cessazione del trattamento va notificata al Garante utilizzando la stessa modulistica usata per la notifica e versando i diritti di segreteria, compilando i soli riquadri a) b) e) h). Naturalmente, se si utilizza il floppy disk, è necessario modificare la precedente copia in possesso del titolare, compilando i riquadri e), h).

BOX 2

SCHEMA IN PDF
[\[cliccare qui per scaricare il file\]](#)

PUNTO 4

Si devono fornire alle persone che possono essere riprese indicazioni chiare, anche se sintetiche, che avvertano della presenza di impianti di videosorveglianza, fornendo anche le informazioni necessarie a sensi dell'art. 10 della legge 675/1996. Ciò è tanto più necessario quando le apparecchiature non siano immediatamente visibili.

Come? Tramite cartelli fissi? Cosa si deve evidenziare nella comunicazione? E' sufficiente dire che l'area è protetta da un impianto TVCC o si devono evidenziare anche i diritti dei visitatori? E se non c'è videoregistrazione resta comunque l'obbligo all'informativa? Anche nel caso di controllo del traffico o del territorio? (Autostrade, centri urbani?)

La legge prevede sempre un'informativa con gli elementi di cui all'art. 10 (vedi box 3), nel modo e nelle forme che il titolare ritiene più agevoli: pertanto è sufficiente un cartello affisso in luogo bene visibile.



BOX 3

Art. 10. Informazioni rese al momento della raccolta

1. (Comma così modificato dall'art. 1, d.lg. 9 maggio 1997, n. 123.) L'interessato o la persona presso la quale sono raccolti i dati personali devono essere previamente informati oralmente o per iscritto circa:

- a) le finalità e le modalità del trattamento cui sono destinati i dati;
- b) la natura obbligatoria o facoltativa del conferimento dei dati;
- c) le conseguenze di un eventuale rifiuto di rispondere;
- d) i soggetti o le categorie di soggetti ai quali i dati possono essere comunicati e l'ambito di diffusione dei dati medesimi;
- e) i diritti di cui all'articolo 13 (**vedi box 4**);
- f) il nome, la denominazione o la ragione sociale e il domicilio, la residenza o la sede del titolare e, se designato, del responsabile.

2. L'informativa di cui al comma 1 può non comprendere gli elementi già noti alla persona che fornisce i dati o la cui conoscenza può ostacolare l'espletamento di funzioni pubbliche ispettive o di controllo, svolte per il perseguimento delle finalità di cui agli articoli 4, comma 1, lettera e), e 14, comma 1, lettera d).

3. Quando i dati personali non sono raccolti presso l'interessato, l'informativa di cui al comma 1 è data al medesimo interessato all'atto della registrazione dei dati o, qualora sia prevista la loro comunicazione, non oltre la prima comunicazione.

4. La disposizione di cui al comma 3 non si applica quando l'informativa all'interessato comporta un impiego di mezzi che il Garante dichiara manifestamente sproporzionati rispetto al diritto tutelato, ovvero si rivela, a giudizio del Garante, impossibile, ovvero nel caso in cui i dati

sono trattati in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria. La medesima disposizione non si applica, altresì, quando i dati sono trattati ai fini dello svolgimento delle investigazioni di cui all'articolo 38 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, approvate con decreto legislativo 28 luglio 1989, n. 271, e successive modificazioni, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento.

Fac-simile di informativa ai sensi dell'art.10

ATTENZIONE!

AREA VIDEOCONTROLLATA!

E' IN FUNZIONE UN IMPIANTO TELEVISIVO

COLLEGATO AD UN DISPOSITIVO DI VIDEOREGISTRAZIONE.

La banca utilizza telecamere per riprendere gli accessi ed eventuali atti illeciti. Le immagini registrate vengono cancellate dopo pochi giorni.

Le immagini sono consultabili solo dall'Autorità Giudiziaria o di Polizia e non sono visionabili dal personale, salvo che per le verifiche del funzionamento del Sistema.

Queste informazioni vengono fornite ai sensi dell'art. 10 della legge 675/1996 e chi entra nei locali accetta di essere ripreso e può esercitare il diritto di accesso, cancellazione, ecc., previsto

dall' art. 13 della Legge n. 675 del 31.12.1996, rivolgendosi al Responsabile del trattamento dei dati personali, Sig. Xxxx Xx Xxxxx, domiciliato per la carica in Via Xxx, Città Xxxx.

Titolare del trattamento dei dati ai sensi della richiamata Legge 675/1996 è la sottoscritta banca Xxx.

La Banca Xxx

BOX 4

Legge n. 675 del 31 dicembre 1996

Tutela delle persone e di altri soggetti rispetto al trattamento

dei dati personali (testo vigente)

Art. 13 - Diritti dell'interessato

1. In relazione al trattamento di dati personali l'interessato ha diritto:

a) di conoscere, mediante accesso gratuito al registro di cui all'articolo 31, comma 1, lettera a), l'esistenza di trattamenti di dati che possono riguardarlo;

b) di essere informato su quanto indicato all'articolo 7, comma 4, lettere a),b) e h);

c) di ottenere, a cura del titolare o del responsabile, senza ritardo:

- la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la comunicazione in forma intelligibile dei medesimi dati e della loro origine, nonché della logica e delle finalità su cui si basa il

trattamento; la richiesta può essere rinnovata, salva l'esistenza di giustificati motivi, con intervallo non minore di novanta giorni;

- la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
- l'aggiornamento, la rettificazione ovvero, qualora vi abbia interesse, l'integrazione dei dati;
- l'attestazione che le operazioni di cui ai numeri 2) e 3) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si riveli impossibile o comporti un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato;

d) di opporsi, in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;

e) di opporsi, in tutto o in parte, al trattamento di dati personali che lo riguardano, previsto a fini di informazione commerciale o di invio di materiale pubblicitario o di vendita diretta ovvero per il compimento di ricerche di mercato o di comunicazione commerciale interattiva e di essere informato dal titolare, non oltre il momento in cui i dati sono comunicati o diffusi, della possibilità di esercitare gratuitamente tale diritto.

2. Per ciascuna richiesta di cui al comma 1, lettera c), numero 1), può essere chiesto all'interessato, ove non risulti confermata l'esistenza di dati che lo riguardano, un contributo spese, non superiore ai costi effettivamente sopportati, secondo le modalità ed entro i limiti stabiliti dal regolamento di cui all'articolo 33, comma 3.

3. I diritti di cui al comma 1 riferiti ai dati personali concernenti persone decedute possono essere esercitati da chiunque vi abbia interesse.

4. Nell'esercizio dei diritti di cui al comma 1 l'interessato può conferire, per iscritto, delega o procura a persone fisiche o ad associazioni.

5. Restano ferme le norme sul segreto professionale degli esercenti la professione di giornalista, limitatamente alla fonte della notizia.

PUNTO 5

Occorre rispettare scrupolosamente il divieto di controllo a distanza dei lavoratori e le precise garanzie previste al riguardo (art. 4, legge 300/1970). Lo Statuto dei lavoratori è citato dalla stessa legge 675/art. 43 (vedi box 5) in modo tale da rendere chiaro il fatto che tale legge resta sempre valida. Pertanto resta fermo il principio di divieto di controllo a distanza dei lavoratori di cui all'art.

E se le esigenze di sicurezza (Security o Safety) sono tali da esigere la ripresa dei lavoratori. Ad esempio nel caso del lavoratore nelle "sale per la conta del denaro" oppure in luoghi a rischio esplosione, dove le riprese sono necessarie per la stessa sicurezza del personale, esiste una deroga? Si devono trovare accordi sindacali con il personale? Ci sono altre strade?

Come accennato sopra, va considerato l'art. 4 nella sua interezza, compreso il comma 2 che, com'è noto, chiarisce i fini e le modalità con cui si può derogare a tale principio. Non si ravvisano altre possibilità per aggirare l'accordo, se non l'intervento della magistratura in un eventuale contenzioso.

Militari e forze dell'ordine sono considerati in modo speciale dallo statuto dei lavoratori?

Certamente militari e forze dell'ordine sono aduse a non ostacolare tecnologie di ausilio alla sicurezza. 4, fermo restando il disposto del comma 2 del medesimo articolo.

BOX 5

Legge n. 675 del 31 dicembre 1996

Tutela delle persone e di altri soggetti rispetto al trattamento

dei dati personali (testo vigente)

Capo IX - Disposizioni transitorie e finali ed abrogazioni (artt. 40 - 43)

Art. 43. Abrogazioni

1. Sono abrogate le disposizioni di legge o di regolamento incompatibili con la presente legge e, in particolare, il quarto comma dell'articolo 8 ed il quarto comma dell'articolo 9 della legge 1° aprile 1981, n. 121. Entro sei mesi dalla data di emanazione del decreto di cui all'articolo 33, comma 1, della presente legge, il Ministro dell'interno trasferisce all'ufficio del Garante il materiale informativo raccolto a tale data in attuazione del citato articolo 8 della legge n. 121 del 1981.

2. Restano ferme le disposizioni della legge 20 maggio 1970, n. 300, e successive modificazioni, nonché, in quanto compatibili, le disposizioni della legge 5 giugno 1990, n. 135, e successive modificazioni, del decreto legislativo 6 settembre 1989, n. 322, nonché le vigenti norme in materia di accesso ai documenti amministrativi ed agli archivi di Stato. Restano altresì ferme le disposizioni di legge che stabiliscono divieti o limiti più restrittivi in materia di trattamento di taluni dati personali.

3. Per i trattamenti di cui all'articolo 4, comma 1, lettera e), della presente legge, resta fermo l'obbligo di conferimento di dati ed informazioni di cui all'articolo 6, primo comma, lettera a), della legge 1° aprile 1981, n. 121.

PUNTO 6

Occorre rispettare i principi di pertinenza e di non eccedenza, raccogliendo solo i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili e limitando l'angolo visuale delle riprese evitando, quando non indispensabili, immagini dettagliate, ingrandite o dettagli non rilevanti, e stabilendo in modo conseguente la localizzazione delle telecamere e le modalità di ripresa.

Ci sono dei limiti più dettagliati? Quali sono i dati "strettamente necessari"? Ad esempio, nelle banche ha senso registrare i "primi piani" dei visitatori: in questo caso sarebbe possibile? Si possono montare telecamere nascoste?

Immagini dettagliate sono quelle che rendono riconoscibile il soggetto; dati strettamente necessari, come dice l'espressione, sono quelli che a me servono per raggiungere il fine che mi ha portato a installare il sistema. Se installo una telecamera per far vedere in rete il tempo che fa nella mia città, è inutile fare dei primi piani ai passanti. Nelle banche ha senso perché l'installazione è stata fatta per fini di sicurezza, dovrò però utilizzare una serie di cautele, come, ad esempio, criteri di sicurezza e crittografia per l'eventuale conservazione del materiale registrato, nonché precise modalità e protocolli per la sua consultazione. Le telecamere, se nascoste, lederebbero il diritto all'informativa.

PUNTO 7

Occorre determinare con precisione il periodo di eventuale conservazione delle immagini, prima della loro cancellazione e prevedere la loro conservazione solo in relazione ad illeciti o a indagini delle autorità giudiziarie o di polizia.

C'è un periodo massimo di conservazione delle immagini? Come si può determinare questo periodo?

Bisogna ricorrere al principio di pertinenza e non eccedenza, pertanto nel caso della banca, una volta verificato che non ci sono stati reati in quel giorno non vi sarebbero motivi per conservare le immagini. Vi sono tendenze, su consiglio della PS, a garantire un'analisi retroattiva delle registrazioni per verificare, in caso di eventi criminosi, la frequentazione dei locali da parte dei sospetti. Il Garante ha comunque indicato un limite temporale logico che non dovrebbe superare i 15 giorni. E' questo il limite adottato anche in altri paesi sottoposti alla Direttiva Comunitaria sulla protezione dei dati personali.

Che diritti ha il visitatore ripreso sui dati registrati? Può pretendere che la sua immagine sia rimossa dal nastro? In quanto tempo?

I diritti dell'interessato riconosciuti dalla legge 675 sono diversi. I principali sono: art.10 - informativa (**vedi box 3**), art. 13 (**vedi box 4**) - chiedere al titolare di conoscere i dati che lo riguardano, di correggerli se errati, di aggiornarli se superati, di cancellarli se raccolti illegittimamente. In caso di mancata risposta o di risposta non ritenuta corretta, l'interessato può rivolgersi con un ricorso ex art. 29 direttamente all'Autorità Giudiziaria o al Garante.

PUNTO 8

Occorre designare per iscritto i soggetti, responsabili e incaricati del trattamento dei dati (art. 8 e 19 della legge 675/1996) che possono utilizzare gli impianti e prendere visione delle registrazioni, avendo cura che essi accedano ai soli dati personali strettamente necessari e vietando rigorosamente l'accesso ad altri soggetti, salvo che si tratti di indagini giudiziarie o di polizia.

Che tipo di responsabilità civili e penali si assumono i soggetti responsabili e l'incaricato del trattamento dei dati? Nel caso di centralizzazione del controllo TVCC presso un istituto di vigilanza nel quale si alternano vari operatori che obblighi sussistono in capo alla guardia giurata od all'istituto?

Le responsabilità possono essere civili o penali a seconda dell'operato del soggetto. Il responsabile o l'incaricato che non esegue le istruzioni impartite dal titolare avrà diverse conseguenze a seconda della violazione eseguita. In materia di misure di sicurezza, ad esempio, la mancata adozione comporta sanzioni penali ex. Art 36 (**vedi box 7**) e civili (risarcimento) ex art. 18/675 (**vedi box 6**).

BOX 6

Art. 18. Danni cagionati per effetto del trattamento di dati personali

Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile.

BOX 7

Legge n. 675 del 31 dicembre 1996

Tutela delle persone e di altri soggetti rispetto al trattamento

dei dati personali (testo vigente)

Capo VIII - Sanzioni (Artt. 34 - 39)

Art. 34. Omessa o infedele notificazione

1. Chiunque, essendovi tenuto, non provvede alle notificazioni prescritte dagli articoli 7 e 28, ovvero indica in esse notizie incomplete o non rispondenti al vero, è punito con la reclusione da tre mesi a due anni. Se il fatto concerne la notificazione prevista dall'articolo 16, comma 1, la pena è della reclusione sino ad anno.

Art. 35. Trattamento illecito di dati personali

1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 11, 20 e 27, è punito con la reclusione sino a due anni o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da tre mesi a due anni.

2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, comunica o diffonde dati personali in violazione di quanto disposto dagli articoli 21, 22, 23 e 24, ovvero del divieto di cui all'articolo 28, comma 3, è punito con la reclusione da tre mesi a due anni.

3. Se dai fatti di cui ai commi 1 e 2 deriva documento, la reclusione è da uno a tre anni.

Art. 36. Omessa adozione di misure necessarie alla sicurezza dei dati

1. Chiunque, essendovi tenuto, omette di adottare le misure necessarie a garantire la sicurezza dei dati personali, in violazione delle disposizioni dei regolamenti di cui ai commi 2 e 3 dell'articolo 15, è punito con la reclusione sino ad un anno. Se dal fatto deriva documento, la pena è della reclusione da due mesi a due anni.

- Se il fatto di cui al comma 1 è commesso per colpa si applica la reclusione fino a un anno.

Art. 37. Inosservanza dei provvedimenti del Garante

1. Chiunque, essendovi tenuto, non osserva il provvedimento adottato dal Garante ai sensi dell'articolo 22, comma 2, o dell'articolo 29, commi 4 e 5, è punito con la reclusione da tre mesi a due anni.

Art. 38. Pena accessoria

1. La condanna per uno dei delitti previsti dalla presente legge importa la pubblicazione della sentenza.

Art. 39. Sanzioni amministrative

1. Chiunque omette di fornire le informazioni o di esibire i documenti richiesti dal Garante ai sensi degli articoli 29, comma 4, e 32, comma 1, è punito con la sanzione amministrativa del pagamento di una somma da lire un milione a lire sei milioni.

2. La violazione delle disposizioni di cui agli articoli 10 e 23, comma 2, è punita con la sanzione amministrativa del pagamento di una somma da lire cinquecentomila a lire tre milioni.

3. (Comma così modificato dall'art. 14, d.lg. 30 luglio 1999, n. 281.) L'organo competente a ricevere il rapporto e ad irrogare le sanzioni di cui al presente articolo è il Garante. Si osservano, in quanto applicabili, le disposizioni della legge 24 novembre 1981, n. 689, e successive modificazioni. I proventi, nella misura del cinquanta per cento del totale annuo, sono riassegnati al fondo di cui all'articolo 33, comma 2, e sono utilizzati unicamente per l'esercizio dei compiti di cui agli articoli 31, comma 1, lettera i) e 32.

PUNTO 9

I dati raccolti per determinati fini (ad esempio, ragioni di sicurezza, tutela del patrimonio) non possono essere utilizzati per finalità diverse o ulteriori (ad esempio, pubblicità, analisi del comportamenti di consumo), salvo le esigenze di polizia o di giustizia e non possono essere diffusi o comunicati a terzi.

Rovesciamo la prospettiva: possono essere installati sistemi TVCC con videoregistrazione con il puro scopo di raccogliere informazioni sul comportamento dei consumatori e comunque non per ragioni di sicurezza? Il fatto che ci sia o meno il riconoscimento dei visitatori modifica le cose? L'eventuale installazione in scuole, ospedali, case di riposo ecc. di telecamere rese disponibili via internet in modo che i famigliari degli ospiti di tali istituti possano vedere i loro congiunti pone problemi di privacy? E L'installazione di web camere a scopo promozionale in centri storici, località turistiche ecc. pone problemi di privacy? Insomma la TVCC si può impiegare solo per ragioni di sicurezza?

Innanzitutto occorre nuovamente distinguere tra TVCC con videoregistratore e sola videoripresa. Ma in questo secondo caso l'esistenza di una diffusione all'esterno del sito sottoposto ad una titolarità fa

nuovamente valere il potere della 675. Solo se i visitatori non sono riconoscibili, neanche indirettamente, non siamo in presenza di trattamento di dati personali. Il fine di marketing è legittimo ma solo se i soggetti sono riconoscibili, e si applica in toto la legge 675 con tutti i vari adempimenti: notifica, informativa ecc. Le telecamere in ospedale pongono certamente un problema in più in quanto finiscono col rilevare informazioni sanitarie e quindi dati sensibili ai sensi dell'art. 22. In questo caso, oltre al consenso dei pazienti e dei loro familiari, è necessaria l'autorizzazione del Garante che deve essere richiesta e ben motivata dalla titolarità.

PUNTO 10

I Particolari impianti per la rilevazione degli accessi dei veicoli ai centri storico e alle zone di traffico limitato devono essere conformi anche alle disposizioni contenute nel D.p.R 250/1999. E' altresì fondamentale che la relativa documentazione sia conservata per il solo periodo necessario per contestare le infrazioni e definire il relativo contenzioso e che ad essa si possa inoltre accedere solo a fini di indagine giudiziaria o di polizia.

Nel caso di controllo del territorio o del traffico, il rischio è di riprendere anche le abitazioni private presenti nell'area oggetto della ripresa. Come affronta il problema il Garante? Solo con la custodia dei dati o anche attraverso l'utilizzo di sistemi che annullino il segnale video in caso di orientamento delle telecamere verso questi target sensibili?

Il Garante ha fornito un parere sulla bozza del D.p.R., reperibile sul sito ufficiale del Garante, per la videosorveglianza per l'accesso ai centri storici, fornendo consigli sul corretto utilizzo di tale strumento per data finalità (**vedi box 8**). Certamente soluzioni hardware o software che consentano di schermare con efficacia eventuali spazi privati e che cadano nel campo di ripresa, debbono essere considerate.

BOX 8

Presidenza del Consiglio dei ministri (Dipartimento funzione pubblica)

OGGETTO: Schema di regolamento per l'autorizzazione all'installazione ed esercizio di impianti per la rilevazione degli accessi di veicoli ai centri storici e alle zone a traffico limitato ai sensi dell'art. 133-bis della legge 15 maggio 1997, n. 127.

Lo schema di regolamento per il quale è stato richiesto il parere del Garante disciplina la rilevazione degli accessi dei veicoli nei centri storici e nelle zone a traffico limitato, anche sulla base di alcune utili disposizioni riferite al trattamento dei dati personali. Il Garante ha constatato con soddisfazione la previsione di tali disposizioni.

La tematica della c.d. videosorveglianza coinvolge infatti uno degli aspetti più delicati della più recente disciplina di tutela della riservatezza, sul quale è necessaria una particolare attenzione.

Il Garante ha ritenuto opportuna la riformulazione di alcune disposizioni, al fine di tener conto dei seguenti principi largamente condivisi nel più recente dibattito europeo sulla materia:

- a)** introdurre sistemi di rilevazione che rilevino immagini solo in caso di infrazione, e che effettuino il monitoraggio del traffico, per il resto, attraverso dati anonimi;
- b)** utilizzazione dei dati per le sole finalità di applicazione delle norme sugli accessi, salva la possibilità di uso dei dati per fini di giustizia e la disponibilità di dati anonimi per studi e statistiche;
- c)** conservazione delle immagini per il periodo necessario all'applicazione delle infrazioni e alla definizione dell'eventuale contenzioso;
- d)** esclusione di interconnessioni con altri archivi o banche dati;
- e)** tracciamento delle consultazioni della banca dati costituita dalle immagini.

Il Garante osserva che la piena osservanza di tali principi non ostacola in alcun modo l'operatività dei controlli e al tempo stesso, però, assicura la doverosa considerazione dei diritti della personalità valorizzando il provvedimento stesso.

Si allegano alcune ipotesi di modifica dello schema, restando a disposizione per ogni ulteriore collaborazione.

IL PRESIDENTE

Artt. 1 e 2 - Nessuna modifica.

Art. 3 - Sostituire il secondo periodo del comma 1 come segue: "Gli impianti raccolgono dati sugli accessi rilevando immagini solo in caso di infrazione". Aggiungere al comma 2 il seguente periodo: "Al verbale non è allegata la documentazione con immagini che è custodita per eventuali contestazioni.". Aggiungere all'inizio del comma 3 le seguenti parole: "La documentazione con immagini è utilizzata per le sole finalità di applicazione del presente regolamento.". Sopprimere la parola: "comunque" inserendo semmai alla fine del medesimo comma le parole: "o di indagine penale". Aggiungere un comma 4 così formulato: "4. La documentazione con immagini è conservata per il solo periodo necessario alla contestazione dell'infrazione e all'applicazione della sanzione.".

Art. 4 - Aggiungere il seguente periodo: "Gli impianti non sono interconnessi con altri impianti, archivi o banche dati.".

Art. 6 - Inserire dopo la parola: "utilizzati" le parole "in forma anonima".

Art. 8 - Introdurre un eventuale termine per l'adeguamento degli impianti già attivi.

STAMPA