

Le nuove norme in tema di videosorveglianza.

Reca la data dell'8 aprile 2010 il provvedimento del Garante della Privacy in materia di videosorveglianza, emanato a seguito delle sempre nuove esigenze di tutela della riservatezza emerse dall'utilizzo di videotecnologie per la tutela della privata proprietà e della pubblica sicurezza. In forza di queste norme, molte imprese saranno chiamate all'adeguamento dei loro sistemi di sorveglianza ai nuovi principi posti dall'Authority, in particolare per gli impatti sulle garanzie previste per i lavoratori nel controllo del loro operato. Ecco in breve i punti cardine del provvedimento.

Proporzionalità: è ammessa la videosorveglianza solo per finalità che sarebbero inattuabili con altri metodi. **Liceità:** per l'utilizzo privato dovrà esservi un reale interesse da tutelare o, per i soggetti pubblici, l'adempimento di scopi istituzionali. **Protezione dei dati:** gli elementi raccolti tramite videosorveglianza dovranno essere custoditi con modalità tali da prevenire qualsiasi impossessamento da parte di terzi o utilizzo per finalità che non siano previste dalla legge. **Informativa:** ogni cittadino che si trovi in spazi sottoposti a procedure di videosorveglianza dovrà essere informato tramite cartelli illustrativi. **Conservazione:** i dati acquisiti potranno essere conservati per un massimo di 24 ore o fino ad una settimana per esigenze d'indagine o pubblica sicurezza.

L'utilizzo di dispositivi di videosorveglianza, sebbene in conformità con il provvedimento dell'Authority, dovranno conformarsi alle innumerevoli altre disposizioni che tutelano l'immagine, il domicilio, la dignità personale in tutti quei luoghi più sensibili a tali valori, (bar, alberghi, palestre, piscine, toilette) senza dimenticare i limiti che lo Statuto dei Lavoratori (Lg. 300/1970), pone al controllo aziendale a distanza nei confronti dei lavoratori.

In sostanza, l'Autorità di vigilanza prendendo atto dell'inevitabile avanzata dei sistemi di video acquisizione, nonché della loro utilità, ha optato per la rigidità dei presupposti d'utilizzo e per gli obblighi d'informazione della loro operatività; quindi, sebbene vi sia un aumento del controllo degli spazi pubblici e privati, parimenti sembra procedere la garanzia per il loro utilizzo.

Dopo una seppur breve panoramica dell'intervento del Garante, doveroso è uno sguardo alle norme più significative del provvedimento pubblicato in Gazzetta Ufficiale n. 99 del 29 Aprile 2010 nonché ai vari ambiti pubblici e privati cui si riferisce il provvedimento *de quo*.

Come detto, rilevante aspetto è l'introduzione di principi fondanti l'utilizzo dello strumento di videosorveglianza: l'immagine rileva, parimenti ad ogni altro dato e informazione personale dotato di sensibilità, ai fini di tutela dei diritti fondamentali della persona. Inoltre la raccolta, la registrazione, la conservazione e, in generale, l'utilizzo di immagini, configura un trattamento di dati personali ai sensi dell'art. 4, comma 1, lett. b), del Codice Privacy.

Per quanto riguarda il requisito della liceità, viene ripresa la categoria già presente nel Codice, ove agli artt. 18-22 per i soggetti pubblici viene richiesta la finalità di svolgimento di compiti istituzionali al fine di poter legittimare un trattamento di dati, mentre per i soggetti pubblici economici e privati si richiamano gli art. 22 e 23 del Codice e i requisiti di adempimento di obblighi di legge, l'ottemperanza ad un provvedimento dello stesso Garante, o la presenza di un consenso libero ed espresso.

Si richiama il principio di necessità dell'art. 3 del Codice, ove si richiede una riduzione al minimo dell'utilizzo di dati personali e la predisposizione dei sistemi di conservazione di tali dati che favoriscano l'anonimato ove ciò sia sufficiente alle finalità previste dall'utilizzo di tali sistemi. Ciò in ottemperanza, altresì, al terzo principio di base, quello di proporzionalità, ossia il bilanciamento tra gli interessi tutelati dall'utilizzo della video acquisizione e la lesione potenziale di diritti soggettivi della persona.

L'Authority non si è preoccupata solamente di incardinare principi in sé poco operativi, ma ha predisposto tassativi adempimenti a carico dei soggetti interessati dall'utilizzo di queste tecnologie.

Rilevanza primaria, vista pure la collocazione iniziale nel testo, ha l'obbligo d'informativa ai terzi della presenza in atto di videosorveglianze.

Il paragrafo 3.1, inerente gli adempimenti necessari, pone chiaramente quale obbligo per il soggetto titolare del sistema di sorveglianza, l'apposizione di uno o più cartelli precedenti il raggio d'azione

della video ripresa, su modello fac-simile allegato al provvedimento e recante l'indicazione obbligatoria del soggetto nominato responsabile della conservazione e trattamento dei dati acquisiti in costanza di tale pratica di video ripresa.

Uniche eccezioni previste sono quelle per finalità di prevenzione e repressione di fenomeni criminosi, in quanto legittimate da specifiche norme di legge e qualora operate da organi afferenti al Dipartimento di Pubblica Sicurezza, per cui in queste situazioni non vige l'obbligo di previa informativa ex art. 53 del Codice. Questo assunto non opera per le video riprese effettuate da privati in collegamento con le forze di polizia, che pertanto richiedono l'informativa al pubblico.

Tra le prescrizioni imposte dal Garante per l'attuazione della disciplina in questione, rilevano gli adempimenti di adeguamento dei sistemi di videoripresa alle disposizioni pubblicate, a carico dei gestori pubblici e privati di tali strutture. Viene prevista una procedura di verifica d'ufficio, o su istanza di parte, di carattere preliminare a cura dell'organo di garanzia, qualora sia il sistema di video ripresa, sia la struttura di conservazione dei dati, possa essere suscettibile di lesione di rilevanti aspetti della sfera soggettiva delle persone e dei diritti fondamentali, come la raccolta di immagini in associazione ad altri dati, per esempio biometrici, o l'utilizzo di sistemi che siano sensibili a determinati comportamenti delle persone, o che effettuino campionamenti di soggetti in relazione a determinate immagini, nonché la necessità di conservazione dei dati acquisiti oltre i termini previsti.

Nei casi in cui invece il sistema di video sorveglianza dovesse attenersi ai requisiti prescritti senza ulteriori ingerenze, la verifica preliminare non risulterebbe necessaria.

Tralasciando gli ulteriori adempimenti richiesti in tema di conservazione dei dati, sia nelle modalità che nelle tempistiche, il provvedimento dell'Authority sottolinea la necessità di coesione con altre norme vigenti in specifici ambiti della vita pubblica e privata, che necessitano di una particolare attenzione per gli interessi coinvolti.

Vale la pena di soffermarsi su questi aspetti e sugli adempimenti che in particolare le realtà aziendali dovranno tenere in considerazione.

Il provvedimento dell'Autorità suddivide le prescrizioni in questi ambiti in tre paragrafi: al numero 5 prevedendo gli adempimenti per i soggetti pubblici, al successivo numero 6 per i soggetti privati e gli enti pubblici economici e al numero 4 per specifici settori d'interesse, ossia ambiti ove emerge più sensibile la tutela di interessi rilevanti per la persona.

Soggetti Pubblici: parimenti ai soggetti privati il provvedimento dell'8 aprile 2010 richiede anche per gli enti pubblici l'adempimento degli obblighi d'informativa nei confronti dei soggetti potenzialmente interessati a tali riprese, salve le esclusioni suddette, qualora il servizio rientri nelle attività tassativamente previste gestite dal Dipartimento per la Pubblica Sicurezza.

Proprio l'ambito della tutela della **sicurezza pubblica** risulta essere quello maggiormente permissivo di deroghe all'obbligo d'informativa previsto nei principi generali, in forza dell'art. 53 del Codice.

Il Garante a tal fine, ribadendo la deroga alle garanzie di riservatezza dei cittadini interessati da tale video sorveglianza, sottolinea il rilevante aumento dell'utilizzo di tali sistemi da parte dei Sindaci e delle altre autorità locali che in forza delle norme di Pubblica Sicurezza rivestono le qualifiche di Autorità di PS o espletano funzioni di PG, richiedendo un coordinamento con le forze di polizia e le direttive del Ministero dell'Interno onde evitare un depauperamento eccessivo della tutela della sfera privata. La problematica sussiste, in questi ambiti nella differenziazione tra esigenze di Sicurezza Pubblica, rientranti nel disposto dell'art. 53 del Codice Privacy che prevede una specifica deroga all'informativa, ed esigenze di Sicurezza Urbana, non definite in alcun modo dal Provvedimento, dove sembra emergere l'obbligo per gli Enti Pubblici di informativa, salvo non si rientri nell'accertamento o nella repressione dei reati che integrerebbe la predetta categoria dell'art. 53 con deroghe annesse. Il principio generale è comunque sempre lo stesso, ossia l'informativa ove possibile, anche in funzione deterrente.

Più strettamente connesso al predetto principio di liceità e necessità, è l'utilizzo dello strumento della video acquisizione d'immagini per la prevenzione e la repressione di illeciti concernenti la violazione delle **norme in tema di rifiuti**, discariche abusive e deposito di rifiuti pericolosi. Il

provvedimento generale in questione, sottolinea ampiamente il requisito della stretta necessità, ossia dell'effettiva utilità dello strumento rispetto alle finalità perseguite e della infruttuosità di altri strumenti prodromici agli stessi fini. Tale aspetto, comunque, emerge quale fattore limitante l'impiego di tali sistemi di sorveglianza, solamente nel caso in cui gli illeciti di cui si intenda effettuare prevenzione o repressione siano meri illeciti amministrativi, (significativo è il richiamo al sistema sanzionatorio della Lg. 689 dell'81), pertanto ove il fatto integri l'estremo dell'illecito penale ritroverebbe applicazione la suddetta previsione derogatoria, con le esclusioni agli obblighi d'informativa annessi *ex art. 53 C. Privacy*.

Altro rilevante aspetto d'interesse oggetto dell'intervento del Garante è l'utilizzo della videosorveglianza per l'accertamento e la contestazione di violazioni alle norme previste in ambito di **circolazione stradale** in quanto, tutta la tipologia di rilevamento automatizzato di infrazioni al CdS, costituisce per l'Authority trattamento di dati personali e, pertanto, risulta interessato dal Provvedimento Generale.

Così l'utilizzo di tali sistemi, in visibile aumento attuale, dovrà essere circoscritto ai principi già più volte enunciati, in particolare alla liceità, quindi nell'ambito dello strettamente necessario al raggiungimento dei fini istituzionali di tutela della sicurezza stradale *ex D. Lgs. 285 del 1992*, e altresì alla proporzionalità, ossia limitando l'acquisizione e la conservazione delle immagini ai dati alfanumerici necessari per identificare il veicolo evitando inutili dettagli ulteriori.

Vale la pena riportare gli adempimenti previsti dal provvedimento del Garante in tale ambito:

1. gli impianti elettronici di rilevamento devono circoscrivere la conservazione dei dati alfanumerici contenuti nelle targhe automobilistiche ai soli casi in cui risultino non rispettate le disposizioni in materia di circolazione stradale;
2. le risultanze fotografiche o le riprese video possono individuare unicamente gli elementi previsti dalla normativa di settore per la predisposizione del verbale di accertamento delle violazioni (*es., ai sensi dell'art. 383 del d.P.R. n. 495/1992, il tipo di veicolo, il giorno, l'ora e il luogo nei quali la violazione è avvenuta*); deve essere effettuata una ripresa del veicolo che non comprenda o, in via subordinata, mascheri, per quanto possibile, la porzione delle risultanze video/fotografiche riguardanti soggetti non coinvolti nell'accertamento amministrativo (*es., pedoni, altri utenti della strada*);
3. le risultanze fotografiche o le riprese video rilevate devono essere utilizzate solo per accertare le violazioni delle disposizioni in materia di circolazione stradale anche in fase di contestazione, ferma restando la loro accessibilità da parte degli aventi diritto;
4. le immagini devono essere conservate per il periodo di tempo strettamente necessario in riferimento alla contestazione, all'eventuale applicazione di una sanzione e alla definizione del possibile contenzioso in conformità alla normativa di settore, fatte salve eventuali esigenze di ulteriore conservazione derivanti da una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria;
5. le fotografie o le immagini che costituiscono fonte di prova per le violazioni contestate non devono essere inviate d'ufficio al domicilio dell'intestatario del veicolo unitamente al verbale di contestazione, ferma restando la loro accessibilità agli aventi diritto;
6. in considerazione del legittimo interesse dell'intestatario del veicolo di verificare l'autore della violazione e, pertanto, di ottenere dalla competente autorità ogni elemento a tal fine utile, la visione della documentazione video-fotografica deve essere resa disponibile a richiesta del destinatario del verbale; al momento dell'accesso, dovranno essere opportunamente oscurati o resi comunque non riconoscibili i passeggeri presenti a bordo del veicolo.

Oltre a questi adempimenti il Garante ribadisce anche, per tali ambiti, l'obbligo generale d'informativa per tutti quei soggetti che si trovino a transitare o accedere alle aree interessate da tali sistemi, sebbene già la normativa di settore ampiamente preveda obblighi di segnalazione anticipata delle postazioni di controllo a distanza o automatizzato al fine della validità della contestazione elevata. Pertanto non sembrano essere state introdotte rilevanti novità o adempimenti a carico delle Amministrazioni interessate.

L'Authority interviene con il provvedimento *de quo* anche nell'ambito privato e degli enti pubblici economici.

Per l'uso privato il Garante, premettendo la non sottoponibilità alla disciplina del Codice qualora si sia in assenza di diffusione a terzi delle immagini rilevate, quindi per i c.d. fini esclusivamente personali, prevede un generico obbligo di cautela per i terzi, per tutti quegli strumenti quali videocitofoni, telecamere interne o condominiali, oppure rilevatori per box auto o per pertinenze d'immobili.

Viene esclusa la possibilità di ripresa video per spazi comuni in sedi condominiali, nonché in spazi antistanti la propria abitazione, anche se non vi sia la conservazione dei dati raccolti, rischiando, in omissione di detto divieto, di incorrere nel reato di interferenza illecita nella vita privata *ex art. 615 bis Cp.* Altresì vengono previsti adempimenti per l'uso privato per fini diversi da quelli esclusivamente personali, sottoponendo tale utilizzo al preventivo consenso dei soggetti interessati dal trattamento dati o agli altri equiparati presupposti del Codice Privacy. In particolare viene esplicitato il principio del bilanciamento degli interessi (p. 6.2.2) che esclude la necessità del previo consenso dei soggetti sottoposti a videosorveglianza solamente qualora l'utilizzo degli strumenti di ripresa video sia prodromica alla tutela di determinati interessi per la raccolta di mezzi di prova, o per la prevenzione di rapine, aggressioni, atti vandalici nonché prevenzione incendi e sicurezza sul lavoro tutto nei termini e alle condizioni previste dal provvedimento.

Come già preannunciato sopra, la disciplina introdotta dall'Organo di Garanzia, vista l'incidenza su aspetti della vita privata di rilevante interesse e di doverosa tutela per le loro basi costituzionali, viene ad inevitabile tangenza con normative già presenti da tempo a disciplinare taluni aspetti ora ripresi in considerazione. Pertanto nella struttura del provvedimento viene data rilevanza a settori di particolare interesse.

Sicuramente di rilievo può essere l'aspetto della videosorveglianza esercitata in **ospedali o in luoghi di cura**, ove il principio fondamentale che viene posto attiene al divieto di diffusione di immagini concernenti soggetti ricoverati in degenza e di persone altresì malate, in modo libero nei confronti del pubblico, ma permettendo tale utilizzo e trattamento di dati solamente per finalità terapeutiche o per i parenti che vogliano vedere il proprio congiunto o nei casi strettamente necessari.

Altresì a requisiti di stretta necessità per la prevenzione di determinati rischi è sottoposto l'utilizzo della videosorveglianza negli **istituti scolastici**, che non deve assolutamente compromettere il diritto alla riservatezza dello studente, ammettendo l'utilizzo in orari notturni o di chiusura e non per il controllo di attività extrascolastiche svolte nei medesimi edifici.

Parimenti, cautele nell'utilizzo di tali tecnologie sono richieste per la loro installazione su **mezzi per il trasporto pubblico** o in prossimità di fermate degli stessi, dovendo sussistere i requisiti di necessità e proporzionalità per il loro impiego e l'obbligo dell'informativa nei confronti degli utenti. L'interesse del Garante si è rivolto anche verso l'utilizzo di webcam per **fini promozionali o turistici**, ove l'unico requisito richiesto è che non sia assolutamente possibile, per il tipo di ripresa effettuato, identificare i dettagli o i soggetti ripresi, data la successiva circolazione di tali immagini sulla rete e la disponibilità *ad libitum* di tali informazioni.

Tralasciando altri aspetti, di primario interesse è l'utilizzo aziendale della videosorveglianza, nonché gli adempimenti che ora le **strutture aziendali** dovranno attuare al fine di posizionarsi sulle nuove linee poste dal Garante.

Fondamentale per la videosorveglianza aziendale è che dovrà essere conforme, oltre alle norme qui espresse, alle disposizioni normative che vietano le attività di controllo a distanza dei lavoratori al fine di effettuare una vigilanza sul dovere di diligenza o sul rispetto degli orari di lavoro pattuiti come previsto dallo Statuto dei Lavoratori.

Qualora la necessità di videosorveglianza aziendale fosse motivata da esigenze di sicurezza o prevenzione per i lavoratori e possa altresì essere suscettibile di controllo sull'operato in via indiretta dei lavoratori, allora tali installazioni dovranno essere previamente concertate con le RSA aziendali o altre rappresentanze interne presenti.

Volendo brevemente riassumere cerchiamo di capire a quali impegni una struttura aziendale dovrà far fronte onde evitare sanzioni dall'Authority:

- *obbligo d'informativa*: con scadenza prevista per il 29 aprile 2011, dovrà essere esposto il cartello informativo ogni qual volta sia attivo un sistema di videosorveglianza anche in orario notturno, e pure in tali ore dovrà essere visibile. Obbligo d'indicare il responsabile del trattamento dei dati, e il dovere di indicare con un apposito cartello i casi in cui i sistemi di ripresa siano collegati con le autorità di pubblica sicurezza,
- in caso di videosorveglianza intelligente o con abbinamento di dati personali vi è l'*obbligo della verifica preliminare* ad opera dell'Autorità di Garanzia.
- *Responsabile del Trattamento*, che obbligatoriamente dovrà essere nominato in ambito aziendale e che avrà la disponibilità dei dati e curerà la loro conservazione.
- Adozione delle *misure di sicurezza* per il trattamento e per la conservazione. Tra le molte si prevede la differenziazione dei ruoli tra gli addetti al trattamento dei dati, il divieto di duplicazione di dati e immagini, l'adozione di procedure che prevedano l'immediata e automatizzata cancellazione dei dati allo scadere dei termini previsti per la conservazione, l'adozione di tecniche crittografiche per la trasmissione dei dati inerenti le immagini acquisite.
- *Notificazione* all'organo di garanzia dei sistemi adottati per la videosorveglianza.
- Rispettare i *termini massimi* di conservazione delle immagini acquisite che non potranno restare nella disponibilità dell'azienda oltre le 24 ore dalla rilevazione.

Verona Aprile 2010,

Dott. Avanzi Marco.