Videosorveglianza
La redazione del regolamento e indicazioni operative

A domanda risponde Avv. Michele IASELLI

23 aprile 2024 - dalle ore 11.30 alle 12.30

ASMEL - Associazione per la Sussidiarietà e la Modernizzazione
degli Enti Locali
Email info@dpoinrete.it
Numero Verde 800.16.56.54
Web: www.dpoinrete.it
www.asmel.eu

Come predisporre un regolamento comunale sulla videosorveglianza

Regolamento per l’installazione e l’utilizzo di telecamere da parte del Comune di……..:

- VISTO il Regolamento UE n. 2016/679 ed il Codice in materia di protezione dei dati personali come modificato ed integrato dal d.lgs. n. 101/2018 ;
- VISTO il "Provvedimento generale sulla videosorveglianza" del Garante per la protezione dei dati personali in data 8 aprile 2010;
- VISTE le linee guida EDPB n. 3/2019 sul trattamento dei dati personali attraverso dispositivi di videosorveglianza del 29 gennaio 2020;
- PRESO ATTO dell’art. 3.1 del "Provvedimento generale sulla videosorveglianza" e di quanto suggerito dalle Linee guida EDPB ai punti 7.1 e seguenti che prevedono:

a) una informativa di primo livello agli interessati che devono essere informati dell’accesso o del transito in una zona videosorvegliata e dell’eventuale registrazione, come da modello semplificato di informativa “minima” individuato dal Garante, da attuarsi mediante cartelli segnalatori;

b) Un’informativa di secondo livello con un avviso circostanziato, che riporti gli elementi dell’art.13 del Regolamento UE n. 2016/679, con particolare riguardo alle finalità e all’eventuale conservazione dei dati raccolti;

Il……

Sentita la relazione del ……. in merito alla necessità di installare e utilizzare delle videocamere dentro e fuori la sede della società,

APPROVA

Il seguente "regolamento per l'installazione e l'utilizzo delle telecamere all'interno e all'esterno del……."

REGOLAMENTO PER L'INSTALLAZIONE E L'UTILIZZO DI TELECAMERE NEL TERRITORIO DEL COMUNE …….

Art. 1
Finalità

Il Comune…… con il progetto di videosorveglianza vuole potenziare gli strumenti in suo possesso per il controllo e la sorveglianza degli accessi, per ragioni di sicurezza. La video sorveglianza è uno strumento di prevenzione e di razionalizzazione dell'azione e degli interventi di chi è preposto a tutelare le esigenze di sicurezza.

Art. 2
Caratteristiche tecniche dell'impianto

Il sistema si compone di una rete di telecamere connesse nella rete intranet del Comune che forniscono immagini alla postazione centrale di controllo degli accessi alle strade comunali. Le immagini possono essere esaminate da remoto, da persone autorizzate, in orari di assenza dal servizio del personale o in giorni festivi, qualora siano stati segnalati allarmi per intrusione, incendio o altro. Le videocamere consentono riprese video anche con scarsa illuminazione notturna. Le immagini saranno visibili presso la postazione centrale di controllo degli accessi al territorio comunale presso ……. Le telecamere sono installate nelle seguenti aree comunali:

Art. 3
Referente/Responsabile della gestione e del trattamento delle immagini.

Il Comune….., ai sensi del Regolamento UE e del d.lgs. n. 196/2003, in qualità di titolare nomina il dott. ……..referente/responsabile della gestione e del trattamento delle immagini (che non sono archiviate). Egli vigila sull'utilizzo dei sistemi e sul trattamento dei dati e delle immagini in conformità agli scopi perseguiti dalla società ed alle altre disposizioni normative che disciplinano la materia ed in particolare alle eventuali disposizioni impartite dall'Autorità Garante per la protezione dei dati personali. Il referente, inoltre, custodisce le chiavi per l'accesso al locale, in cui sono collocati i server che gestiscono la rete informatica del Comune e le parole chiave per l'utilizzo dei sistemi. Il…….. designa e nomina i soggetti autorizzati a cui affida i compiti specifici e le prescrizioni per l'utilizzo dei sistemi. Alle immagini in diretta provenienti dalle varie videocamere possono accedere soltanto i dipendenti che prestano servizio nella postazione di controllo dell'accesso principale del Comune.

Per l'esercizio dei diritti di cui al regolamento UE, il cittadino potrà rivolgersi al referente della gestione e del trattamento dei dati, presso il Comune, nel rispetto di quanto prescritto dal Regolamento UE n. 2016/679 e dal Codice in materia di protezione dei dati personali.

Art. 4
Principio di minimizzazione dei dati

Il trattamento effettuato mediante il sistema di videosorveglianza del Comune……. sarà improntato, in linea con la normativa in materia di protezione dei dati personali, ai principi di correttezza, pertinenza e minimizzazione dei dati, liceità, necessità, proporzionalità e limitazione delle finalità e nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità delle persone, con particolare riferimento alla tutela della riservatezza, alla identità personale e al diritto alla protezione dei dati personali delle persone, come prescritto dal provvedimento del Garante per la protezione dei dati personali del 08/04/2010.

Con riferimento ai principi di pertinenza e minimizzazione dei dati trattati rispetto agli scopi perseguiti, le telecamere saranno installate in modo tale da limitare l'angolo visuale delle riprese, evitando quando non indispensabili come nell'ipotesi di cui al successivo art. 6 immagini dettagliate, ingrandite o dettagli non rilevanti per non consentire la ripresa dei tratti somatici delle persone e di qualunque altro dettaglio idoneo alla loro identificazione,

E' comunque vietato divulgare o diffondere immagini, dati e notizie di cui si è venuti a conoscenza nell'utilizzo degli impianti, nonché procedere a qualsiasi ingrandimento delle immagini al di fuori dei casi regolati dal presente regolamento. E' vietato utilizzare le immagini che anche accidentalmente dovessero essere assunte, per finalità di controllo anche indiretto sull'attività professionale dei dipendenti, secondo il disposto dell'art. 4 della Legge 20/05/1970 n. 300 (Statuto dei Lavoratori), e ferma restando la procedura prevista dal medesimo articolo.

Per quanto non risulti disciplinato dal presente documento, si rinvia a quanto disposto dal Regolamento UE n. 2016/679 ed ai provvedimenti a carattere generale del Garante per la protezione dei dati personali.

Art. 5
Accertamenti di illeciti e indagini di Autorità Giudiziarie o di Polizia.

L'incaricato della videosorveglianza potrà provvedere a registrare le immagini e a darne immediata comunicazione al titolare/referente qualora le immagini contengano fatti che possono portare ad ipotesi di reato o ad eventi rilevanti ai fini della sicurezza pubblica o della tutela ambientale. In tali casi, in deroga o quanto prescritto nelle modalità di ripresa definita dal precedente art. 4, l'incaricato potrà procedere agli ingrandimenti della ripresa delle immagini strettamente necessari e non eccedenti allo specifico scopo perseguito ed alla registrazione delle stesse su supporti magnetici. Alle informazioni raccolte ai sensi del presente articolo possono accedere solo gli organi di Polizia e l'Autorità Giudiziaria dietro specifica richiesta. Le immagini potranno essere utilizzate anche in relazione ad indagini di Autorità Giudiziaria o di Polizia.

Art. 6

Conservazione delle immagini e custodia dei supporti magnetici od ottici.

I supporti su cui sono archiviate le immagini di cui all'articolo 5 dal referente o dai soggetti autorizzati, numerati e registrati sono conservati in idonea cassetta di sicurezza le cui chiavi saranno in possesso dei soggetti di cui al precedente art. 3. Ad essi inoltre, compete la tenuta di un idoneo registro in cui dovranno essere annotati la data della registrazione e quella di cancellazione dell'immagine e la firma degli incaricati che hanno effettuato operazioni normate dal presente regolamento.

Le registrazioni sono messe a disposizione dell'Autorità Giudiziaria o di altre pubbliche Autorità solo in presenza di provvedimenti da queste emanati.

La cancellazione delle immagini dai supporti dovrà avvenire con gli strumenti tecnologicamente più rapidi e sicuri da parte degli incaricati, previa autorizzazione scritta del referente.

Le immagini eventualmente registrate in base all'articolo 5 devono essere immediatamente cancellate se il titolare/referente non ritiene di darne informazione agli organi di Polizia o all'Autorità Giudiziaria.

Art. 7
Informativa

Il Comune…… con idonea cartellonistica e specifiche comunicazioni informerà dell'esistenza del servizio di videosorveglianza, fornendo anche l'indicazione del referente a cui potranno rivolgersi i cittadini per l'esercizio dei diritti di cui al Regolamento UE.

Il presente regolamento sarà pubblicato ……..e una copia dello stesso potrà essere richiesta presso……...

Il presente avviso in formato integrale viene pubblicato nel sito Internet del Comune ……..

Copia dello stesso può essere richiesto presso il titolare o al referente del trattamento dei dati, nonché presso l'ufficio……... Il medesimo avviso potrà essere integrato o modificato con successivo provvedimento, in caso di variazione delle condizioni di applicazione.

Art. 8
Disposizioni attuative e di rinvio

Per tutto quanto non risulti disciplinato nel presente regolamento, si rinvia a quanto disposto dal Regolamento UE n. 2016/679, alle linee guida EDPB n. 3/2019 ed al provvedimento a carattere generale del Garante per la protezione dei dati personali dell’8 aprile 2010..

La divulgazione di filmati video a terzi

Per divulgazione si intende la trasmissione (ad es. comunicazione individuale), la diffusione (ad es. pubblicazione online) o la messa a disposizione in altro modo.

L'eventuale comunicazione di dati personali costituisce un tipo di trattamento distinto di dati personali per il quale il titolare del trattamento deve avere una base giuridica nell'articolo 6.
Pensiamo ad esempio ad un titolare del trattamento che desidera caricare una registrazione su Internet e deve basarsi su una base giuridica per tale trattamento, ad esempio ottenendo il consenso dell'interessato ai sensi dell'articolo 6, paragrafo 1, lettera a).

La trasmissione di filmati video a terzi per scopi diversi da quello per cui sono stati raccolti i dati è possibile ai sensi dell'articolo 6, paragrafo 4.
In particolare il titolare del trattamento dovrà tener conto:

a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto;
b) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento;
c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'articolo 9, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10;
d) delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;
e) dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione.

Anche la divulgazione delle registrazioni video alle forze dell'ordine è un processo indipendente, che richiede una giustificazione separata per il controllore.
Ai sensi dell'articolo 6, paragrafo 1, lettera c), il trattamento è legale se è necessario per l'adempimento di un obbligo legale al quale è soggetto il titolare del trattamento.
Se, quindi, la legislazione nazionale impone al titolare del trattamento di cooperare con le forze dell'ordine (ad es. indagini), la base giuridica per la trasmissione dei dati è l'obbligo giuridico di cui all'articolo 6, paragrafo 1, lettera c).

RICHIESTA DI ACCESSO ALLE IMMAGINI DELLA VIDEOSORVEGLIANZA

Al Designato al Trattamento dei Dati Personali di Videosorveglianza
Comune di _____
E-mail: _____
Pec: _____

Oggetto: RICHIESTA DI ACCESSO ALLE IMMAGINI DELLA VIDEOSORVEGLIANZA

Il/La Sottoscritto/a_____, nato/a a _____ il _____, codice fiscale _____, residente a _____ in _____, tel. _____, indirizzo e-mail/pec _____.

In qualità di Interessato (oppure da specificare soltanto nel caso in cui il richiedente agisca in qualità di pubblico ufficiale o per procura legale o quale rappresentate di soggetto giuridico, in tal caso indicare i riferimenti dell'interessato)

_____
_____
_____
_____

Consapevole che l'esercizio del diritto d'accesso presuppone un interesse diretto, concreto e attuale corrispondente ad una situazione giuridicamente tutelata e che l'accesso ai dati personali deve essere limitato, pertinente e proporzionale alla finalità del trattamento, ai sensi del Regolamento UE n. 679/2016 e del Dlgs 196/2003.

CHIEDE

di prendere visione delle immagini registrate dagli impianti di videosorveglianza dell'Ente il giorno _____ dalle ore _____ alle ore _____ presso _____

Per la motivazione di:

_____
_____
_____
_____
_____
_____

A tal fine allega:

1. Documento d'identità;
2. _____
3. _____

Si prende visione della seguente dell'informativa breve sulla privacy:
In ottemperanza a quanto prevede la normativa sulla privacy, Regolamento UE n. 679/2016 (GDPR) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati e dlgs n. 196/2003, Codice in materia di protezione dei dati personali, così come aggiornato dal dlgs n. 101/2018, si informa che tutti i dati personali, comprese eventualmente le c.d. "categorie particolari" di cui all'art. 9 del GDPR, vengono acquisiti per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, per le finalità e nell'ambito dello svolgimento dei presenti servizi, ovvero la richiesta di accesso agli atti, che tali dati saranno trattati unicamente dai soggetti autorizzati e per l'espletamento delle attività in oggetto in conformità a quanto previsto dalla normativa sopra richiamata, che in ogni momento possono essere esercitati i diritti sui propri dati scrivendo ai seguenti contatti E-mail: _____ Pec: _____, che l'informativa estesa contenente tutte le informazioni previste sul trattamento dei dati personali è pubblicata e visionabile sul seguente sito web: _____.

Luogo _____, data _____

Firma

_____

Attestazione di esercizio del diritto d'accesso

Il/La Sottoscritto/a_____, in qualità di _____ dichiara che in data _____ la richiesta di acceso ai dati di cui sopra:

- ❑ è stata accolta e soddisfatta;
- ❑ non è stata accolta per le seguenti motivazioni

_____
_____
_____
_____
_____
_____

Firma

_____

Precauzioni da adottare nel caso di videosorveglianza intelligente.

Come è noto la videosorveglianza è diventata altamente performante grazie alla crescente implementazione dell'analisi video intelligente. Queste tecniche possono essere più intrusive (ad es. tecnologie biometriche complesse) o meno intrusive (ad es. semplici algoritmi di conteggio). Rimanere anonimi e preservare la propria privacy è in generale sempre più difficile. I problemi di protezione dei dati sollevati in ogni situazione possono differire, così come l'analisi legale quando si utilizza l'una o l'altra di queste tecnologie.

Per videosorveglianza intelligente s’intende, in particolare, quel sistema di video controllo associato ad altri software in grado di generare sistemi integrati ad alta funzionalità, dal punto di vista della sicurezza aziendale.

Un sistema di videosorveglianza intelligente non si limita a rilevare e/o registrare immagini ma esegue una video analisi, ottimizzandone il risultato finale. Altamente performante dal punto di vista tecnologico, il riconoscimento facciale, la direzione di movimento veicoli e persone, l' attraversamento di zone cui è vietato l'accesso e lo scavalcamento di recinzioni, sono solo alcuni esempi di cosa possa essere captato e gestito, nello stesso arco temporale.

Inoltre, l'applicazione di telecamere termografiche in particolari condizioni di criticità, permettono di operare anche in ambienti con scarsa illuminazione, fornendo il controllo assoluto su siti particolarmente a rischio. Monitorare e generare un' allerta automatico in caso di incidente o anomalia, per determinate categorie industriali risulta essere di vitale importanza.

Ricordiamo con grande amarezza i disastri ambientali e la perdita di vite umane verificatesi nell'ultimo decennio, soprattutto negli impianti petroliferi. Se ciò è accaduto è anche perché non eravamo sufficientemente protetti.
La rivoluzione e l'applicazione di strumenti intelligenti hanno innalzato notevolmente il livello di guardia.

L’analisi video

L’avvento del digitale, oltre a garantire l’alta definizione delle immagini unita alla facilità di installazione e versatilità di utilizzo, ha reso possibile lo sviluppo del concetto di analisi video. Il collegamento in rete dei sistemi di videosorveglianza consente infatti l’utilizzo di software che esaminano le riprese, riconoscendo in automatico eventuali criticità.

L’ analisi video permette diversi tipi di applicazione:

- Rilevamento di movimento, grazie al quale la registrazione ha inizio solo nel momento in cui viene accertata una variazione significativa nel contenuto delle riprese. Questa applicazione consente di risparmiare sui tempi di registrazione e sui costi di archiviazione delle immagini;
- Rilevamento di intrusi e riconoscimento di volti umani e oggetti in movimento. Tale strumento si rivela molto utile laddove si svolgono attività che richiedono il monitoraggio di persone o veicoli;
- Rilevamento di oggetti abbandonati o smarriti, fondamentale per controllare beni di valore o individuare la presenza di oggetti potenzialmente pericolosi.

Ciò che fino a poco tempo fa sembrava fantascienza, oggi è pane quotidiano per chi si occupa di sistemi di sicurezza. Ne è la conferma il fatto che tutte le più grandi aziende del settore stanno investendo nello sviluppo di software di videoanalisi sempre più performanti.

I dati biometrici

Le linee guida sostengono che l'utilizzo di dati biometrici e in particolare il riconoscimento facciale comportano rischi maggiori per i diritti delle persone interessate.
È, quindi, fondamentale che il ricorso a tali tecnologie avvenga nel rispetto dei principi di legalità, necessità, proporzionalità e minimizzazione dei dati, come stabilito dal GDPR.
Mentre l'uso di queste tecnologie può essere percepito come particolarmente efficace, i titolari del trattamento dovrebbero prima di tutto valutare l'impatto sui diritti e sulle libertà fondamentali e considerare mezzi meno invasivi per raggiungere il loro legittimo scopo del trattamento.

Per parlare di dato biometrico alla luce degli articoli 4.14 e 9 del GDPR, si devono considerare tre criteri:

- **Natura dei dati:** dati relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica;
- **Mezzi e modalità di elaborazione**: dati "risultanti da un'elaborazione tecnica specifica";
- **Scopo del trattamento:** i dati devono essere utilizzati per identificare in modo univoco una persona fisica.

L'articolo 9 del GDPR si applica se il titolare del trattamento memorizza dati biometrici (più comunemente attraverso modelli creati mediante l'estrazione di caratteristiche chiave dalla forma grezza dei dati biometrici (ad es. misurazioni facciali da un'immagine)) al fine di identificare in modo univoco una persona.

Se un titolare del trattamento desiderasse rilevare un soggetto che rientra nell'area o che entra in un'altra area (ad esempio per proiettare un annuncio pubblicitario personalizzato), lo scopo sarebbe quello di identificare in modo univoco una persona fisica, il che significa che l'operazione rientrerebbe fin dall'inizio nell'ambito di applicazione dell'articolo 9.

Talvolta alcuni sistemi biometrici sono installati in ambienti non controllati, il che significa che il sistema prevede la cattura al volo dei volti di qualsiasi individuo che passa nel raggio d'azione della telecamera, comprese le persone che non hanno acconsentito al dispositivo biometrico, e quindi la creazione di modelli biometrici. Questi modelli vengono confrontati con quelli creati da persone che hanno dato il loro previo consenso durante un processo di arruolamento (cioè un utente biometrico) affinché il titolare del trattamento dei dati riconosca se la persona è un utente di dispositivi biometrici o meno.
In questo caso, il sistema è spesso progettato per discriminare gli individui che vuole riconoscere da un database da quelli che non sono arruolati ed ovviamente è necessaria una specifica eccezione ai sensi dell'art. 9 paragrafo 2 del GDPR.

Quando il trattamento biometrico viene utilizzato a scopo di autenticazione, il titolare del trattamento deve offrire una soluzione alternativa che non comporti un trattamento biometrico - senza restrizioni o costi aggiuntivi per la persona interessata. Questa soluzione alternativa è necessaria anche per le persone che non rispettano i vincoli del dispositivo biometrico (iscrizione o lettura dei dati biometrici impossibile, situazione di disabilità che ne rende difficile l'utilizzo, ecc.) e in previsione di una indisponibilità del dispositivo biometrico (come un malfunzionamento del dispositivo), deve essere implementata una "soluzione di back-up" per garantire la continuità del servizio proposto, limitata però ad un uso eccezionale.

L'identificazione e l'autenticazione/conversione richiederanno probabilmente la memorizzazione del modello per un successivo confronto. Il titolare del trattamento dei dati deve considerare il luogo più appropriato per la memorizzazione dei dati.
In un ambiente sotto controllo (corridoi delimitati o checkpoint), i template devono essere memorizzati su un singolo dispositivo tenuto dall'utente e sotto il suo unico controllo (in uno smartphone o nella carta d'identità) o - quando necessario per scopi specifici e in presenza di esigenze oggettive - memorizzati in un database centralizzato in forma criptata con una chiave/segreta nelle sole mani della persona per impedire l'accesso non autorizzato al template o al luogo di memorizzazione.

Naturalmente in conformità al principio di minimizzazione dei dati, i titolari del trattamento devono garantire che i dati estratti da un'immagine digitale per costruire un modello non siano eccessivi e contengano solo le informazioni necessarie per lo scopo specificato, evitando così ogni possibile ulteriore elaborazione.

Dal punto di vista tecnico il titolare del trattamento deve adottare tutte le precauzioni necessarie per preservare la disponibilità, l'integrità e la riservatezza dei dati trattati.
A tal fine deve:

1. compartimentare i dati durante la trasmissione e la memorizzazione;
2. memorizzare i modelli biometrici e i dati grezzi o i dati di identità su database distinti;
3. cifrare i dati biometrici, in particolare i modelli biometrici, e definire una politica di cifratura e di gestione delle chiavi;
4. integrare una misura organizzativa e tecnica per l'individuazione delle frodi;
5. associare un codice di integrità ai dati (ad esempio firma o hash) e vietare qualsiasi accesso esterno ai dati biometrici.

Tali misure naturalmente dovranno evolvere con il progresso delle tecnologie.

Misure tecniche ed organizzative

Le linee guida ricordano che come stabilito dall'articolo 32, paragrafo 1, del GDPR, il trattamento dei dati personali durante la videosorveglianza non solo deve essere legalmente consentito, ma i titolari del trattamento e gli incaricati del trattamento devono anche proteggerli adeguatamente.
Le misure organizzative e tecniche attuate devono essere **proporzionate ai rischi per i diritti e le libertà delle persone fisiche**, derivanti da distruzione accidentale o illecita, perdita, alterazione, divulgazione non autorizzata o accesso ai dati di videosorveglianza.
Ai sensi degli articoli 24 e 25 del GDPR, i titolari del trattamento devono attuare misure tecniche e organizzative anche al fine di salvaguardare tutti i principi di protezione dei dati durante il trattamento e stabilire i mezzi per l'esercizio dei diritti degli interessati, come definiti negli articoli 15-22 del GDPR.

Principio della privacy by design e by default

Le linee guida ricordano che i titolari del trattamento devono attuare misure tecniche e organizzative adeguate per la protezione dei dati non appena pianificano la videosorveglianza - prima di iniziare la raccolta e l'elaborazione delle riprese video.
Questi principi sottolineano la necessità di tecnologie integrate per migliorare la privacy, di impostazioni predefinite che riducano al minimo il trattamento dei dati e di fornire gli strumenti necessari che consentano la massima protezione possibile dei dati personali.

I titolari del trattamento dovrebbero integrare la protezione dei dati e la tutela della vita privata non solo nelle specifiche di progettazione della tecnologia, ma anche nelle pratiche organizzative.
Quando si tratta di pratiche organizzative, il controllore dovrebbe adottare un quadro di gestione adeguato, stabilire e applicare politiche e procedure relative alla videosorveglianza.

Nella scelta delle soluzioni tecniche, il controllore dovrebbe considerare tecnologie rispettose della privacy anche perché migliorano la sicurezza.
Esempi di tali tecnologie sono i sistemi che consentono di mascherare o rimescolare aree che non sono rilevanti per la sorveglianza, o il montaggio di immagini di terze persone, quando si forniscono riprese video ai soggetti interessati.
D'altra parte, le soluzioni selezionate non dovrebbero fornire funzioni che non siano necessarie (ad esempio, movimento illimitato delle telecamere, capacità di zoom, trasmissione radio, analisi e registrazioni audio). Le funzioni fornite, ma non necessarie, devono essere disattivate.

Con riferimento alle misure tecniche le linee guida rinviano a quanto disposto dall'art. 32 del GDPR ed inoltre distinguono tra:

- **Sicurezza fisica**: una parte vitale della protezione dei dati e la prima linea di difesa, perché protegge le apparecchiature VSS da furti, atti vandalici, catastrofi naturali, catastrofi antropiche e danni accidentali (ad esempio, da sovratensioni elettriche, temperature estreme e caffè versato). Nel caso di sistemi analogici, la sicurezza fisica gioca il ruolo principale nella loro protezione.
- **Sicurezza del sistema e dei dati**, cioè la protezione contro interferenze intenzionali e non intenzionali con il normale funzionamento che può includere:
  - Protezione dell'intera infrastruttura VSS (comprese le telecamere remote, il cablaggio e l'alimentazione) contro manomissioni fisiche e furti.
  - Protezione della trasmissione di filmati con canali di comunicazione sicuri contro le intercettazioni.
  - Crittografia dei dati.
  - Utilizzo di soluzioni basate su hardware e software come firewall, antivirus o sistemi di rilevamento delle intrusioni contro gli attacchi informatici.
  - Rilevamento di guasti di componenti, software e interconnessioni.
  - Mezzi per ripristinare la disponibilità e l'accesso al sistema in caso di incidente fisico o tecnico.
- **Controllo degli accessi** il quale assicura che solo le persone autorizzate possano accedere al sistema e ai dati, mentre ad altri è impedito l'accesso.

Dal punto di vista organizzativo a parte una potenziale DPIA necessaria, le linee guida consigliano ai titolari di approfondire i seguenti argomenti quando creano le proprie politiche e procedure di videosorveglianza:

- individuazione del responsabile della gestione e del funzionamento del sistema di videosorveglianza.
- Scopo e portata dell'impianto di videosorveglianza.
- Uso appropriato e vietato (dove e quando la videosorveglianza è consentita e dove e quando non lo è).
- Misure di trasparenza.
- Come viene registrato il video e per quale durata, compresa l'archiviazione delle registrazioni video relative agli incidenti di sicurezza.
- Chi deve seguire una formazione pertinente e quando.
- Chi ha accesso alle registrazioni video e per quali scopi.
- Procedure operative (ad es. da chi e da dove viene monitorata la videosorveglianza, cosa fare in caso di violazione dei dati).
- Quali sono le procedure che i soggetti esterni devono seguire per richiedere le registrazioni video e le procedure per negare o concedere tali richieste.
- Procedure per l'approvvigionamento, l'installazione e la manutenzione dei VSS.
- Gestione degli incidenti e procedure di recupero.

FAQ GARANTE

DOMANDE