Videosorveglianza - linee guida e gestione del contenzioso

A domanda risponde Prof. Avv. Michele IASELLI

8 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

Per le ovvie implicazioni in materia di protezione dei dati personali la videosorveglianza, al di là dei principi generali dettati dal Regolamento UE n. 2016/679, è disciplinata dalle linee guida EDPB n. 3/2019 sul trattamento dei dati personali attraverso dispositivi di videosorveglianza e dal provvedimento generale del nostro Garante sulla videosorveglianza datato 8 aprile 2010 laddove compatibile con la normativa comunitaria.

Perché delle linee guida?

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.

Oltre ai problemi di privacy, vi sono anche rischi legati a possibili malfunzionamenti di questi dispositivi e ai pregiudizi che possono indurre. I ricercatori riferiscono che il software utilizzato per l'identificazione facciale, il riconoscimento o l'analisi si comporta in modo diverso in base all'età, al sesso e all'etnia della persona che sta identificando.

Per questo motivo, i titolari del trattamento devono anche assicurare che il trattamento dei dati biometrici derivanti dalla videosorveglianza sia sottoposto a una valutazione periodica della sua rilevanza e dell'adeguatezza delle garanzie fornite.

La videosorveglianza non è di default una necessità quando ci sono altri mezzi per raggiungere lo scopo della sicurezza. Altrimenti rischiamo un cambiamento delle norme culturali che porti all'accettazione della mancanza di privacy come impostazione iniziale.

Le linee guida, quindi, hanno lo scopo di fornire indicazioni su come applicare il GDPR in relazione al trattamento dei dati personali attraverso dispositivi video.

Campo di applicazione

Il monitoraggio sistematico e automatizzato di un determinato spazio con mezzi ottici o audiovisivi, per lo più a scopo di protezione della proprietà, o per proteggere la vita e la salute dell'individuo, è diventato un fenomeno significativo dei nostri giorni.
Questa attività comporta la raccolta e la conservazione di immagini o informazioni audiovisive relative a tutte le persone che entrano nello spazio monitorato, identificabili in base al loro aspetto o ad altri elementi specifici.

Questo fatto è rispecchiato dal regolamento generale sulla protezione dei dati nell'articolo 35, paragrafo 3, lettera c), che impone l'esecuzione di una valutazione d'impatto sulla protezione dei dati in caso di monitoraggio sistematico di uno spazio accessibile al pubblico su vasta scala, nonché nell'articolo 37, paragrafo 1, lettera b), che impone ai titolari o responsabili del trattamento di designare un responsabile della protezione dei dati, se il trattamento per sua natura comporta un monitoraggio regolare e sistematico delle persone interessate.

Liceità del trattamento

La videosorveglianza può servire a molti scopi, ad esempio sostenere la protezione della proprietà e di altri beni, sostenere la protezione della vita e dell'integrità fisica degli individui, raccogliere prove per le cause civili.
Questi scopi di monitoraggio devono essere documentati per iscritto (articolo 5, paragrafo 2) e devono essere specificati per ogni telecamera di sorveglianza in uso. Le telecamere che vengono utilizzate per lo stesso scopo da un unico controllore possono essere documentate insieme. Inoltre, gli interessati devono essere informati delle finalità del trattamento ai sensi dell'articolo 13.

Sostengono le linee guida che in linea di principio, ogni motivo giuridico ai sensi dell'articolo 6, paragrafo 1, può fornire una base giuridica per l'elaborazione dei dati di videosorveglianza.
Ad esempio, l'articolo 6, paragrafo 1, lettera c), si applica quando la legislazione nazionale prevede l'obbligo di effettuare la videosorveglianza. Tuttavia, nella pratica, le disposizioni più probabili da utilizzare sono:

- Articolo 6, paragrafo 1, lettera f) (interesse legittimo),
- Articolo 6, paragrafo 1, lettera e) (necessità di svolgere un compito di interesse pubblico o nell'esercizio di pubblici poteri).

In casi piuttosto eccezionali, l'articolo 6, paragrafo 1, lettera a) (consenso) potrebbe essere utilizzato come base giuridica dal titolare del trattamento.

Riguardo l’interesse legittimo, le linee guida puntualizzano che la videosorveglianza è legale se è necessaria per soddisfare lo scopo di un interesse legittimo perseguito da un titolare del trattamento o da un terzo, a meno che tali interessi non siano superati dagli interessi dell'interessato o dai diritti e dalle libertà fondamentali (articolo 6, paragrafo 1, lettera f)).
Gli interessi legittimi perseguiti da un controllore o da un terzo possono essere interessi legali, economici o non materiali. Tuttavia, il titolare del trattamento deve considerare che se l'interessato si oppone alla sorveglianza ai sensi dell'articolo 21, può procedere alla videosorveglianza dell'interessato solo se si tratta di un interesse legittimo prevalente su altri interessi, diritti e libertà dell'interessato o per l'accertamento, l'esercizio o la difesa di diritti legali.

E’ quindi obbligatorio secondo le linee guida che venga sempre effettuato un bilanciamento degli interessi.
I diritti e le libertà fondamentali, da un lato, e i legittimi interessi del controllore, dall'altro, devono essere valutati ed equilibrati con attenzione.
Le decisioni dovranno essere prese caso per caso considerando le ragionevoli aspettative dell'interessato al momento e nel contesto del trattamento dei suoi dati personali.

Per quanto riguarda il monitoraggio sistematico, il rapporto tra l'interessato e il titolare del trattamento può variare in modo significativo e può influire sulle ragionevoli aspettative dell'interessato.
Ad esempio, nella maggior parte dei casi un dipendente sul posto di lavoro non si aspetta di essere monitorato dal suo datore di lavoro.
Inoltre, il monitoraggio non è previsto nel giardino privato, negli spazi abitativi o nelle sale per esami e trattamenti. Allo stesso modo, non è ragionevole aspettarsi un monitoraggio negli impianti sanitari o nelle saune - il monitoraggio di tali aree è un'intensa intrusione nei diritti della persona interessata. La ragionevole aspettativa degli interessati è che non si verifichi alcuna videosorveglianza in quelle aree.

Le linee guida affrontano anche la questione della necessità del trattamento per quanto riguarda le modalità di conservazione delle prove.
In alcuni casi potrebbe essere necessario utilizzare soluzioni di scatola nera in cui le riprese vengono automaticamente cancellate dopo un certo periodo di conservazione e accessibili solo in caso di incidente. In altre situazioni, potrebbe non essere necessario registrare il materiale video, ma è più appropriato utilizzare il monitoraggio in tempo reale.
Anche la decisione tra soluzioni con scatola nera e monitoraggio in tempo reale dovrebbe essere basata sullo scopo perseguito.
Se ad esempio lo scopo della videosorveglianza è la conservazione delle prove, i metodi in tempo reale di solito non sono adatti.
Viene ricordato che a volte il monitoraggio in tempo reale può anche essere più intrusivo rispetto alla memorizzazione e alla cancellazione automatica del materiale dopo un periodo di tempo limitato.

Riguardo la configurabilità della base giuridica del consenso abbiamo visto che le linee guida la vedono come remota in quanto la videosorveglianza monitora un numero imprecisato di persone contemporaneamente, per cui il titolare del trattamento difficilmente potrà dimostrare che l'interessato ha dato il suo consenso prima del trattamento dei suoi dati personali.
Inoltre in considerazione dello squilibrio di potere tra datori di lavoro e dipendenti, nella maggior parte dei casi i datori di lavoro non dovrebbero fare affidamento sul consenso per il trattamento dei dati personali, in quanto è improbabile che venga dato liberamente.

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).

Trattamento di particolari categorie di dati

Le linee guida precisano che i sistemi di videosorveglianza raccolgono di solito quantità massicce di dati personali che possono rivelare dati di natura altamente personale e anche categorie particolari di dati.
In effetti, dati apparentemente non significativi originariamente raccolti attraverso il video possono essere utilizzati per dedurre altre informazioni per raggiungere uno scopo diverso (ad esempio, per mappare le abitudini di un individuo).
Tuttavia, la videosorveglianza non è sempre considerata come trattamento di particolari categorie di dati personali.

In generale, in linea di principio, ogni volta che si installa un sistema di videosorveglianza si dovrebbe considerare attentamente il principio della minimizzazione dei dati.
Pertanto, anche nei casi in cui non si applica l'articolo 9, paragrafo 1, il titolare del trattamento dovrebbe sempre cercare di ridurre al minimo il rischio di catturare filmati che rivelino altri dati sensibili (oltre all'articolo 9), indipendentemente dalla finalità.

Se per il trattamento di categorie particolari di dati viene utilizzato un sistema di videosorveglianza, il titolare del trattamento deve individuare sia un'eccezione per il trattamento di categorie particolari di dati ai sensi dell'articolo 9 (ossia un'esenzione dalla regola generale secondo cui non si devono trattare categorie particolari di dati), sia una base giuridica ai sensi dell'articolo 6 del GDPR.

I diritti degli interessati

Diritto di accesso

Per la videosorveglianza l’esercizio del diritto di accesso da parte dell’interessato comporta che se nessun dato viene memorizzato o trasferito in alcun modo, una volta trascorso il momento di monitoraggio in tempo reale, il titolare del trattamento può solo dare l'informazione che nessun dato personale è più oggetto di trattamento (oltre agli obblighi generali di informazione di cui all'articolo 13 GDPR).
Se tuttavia i dati sono ancora in corso di trattamento al momento della richiesta (cioè se i dati sono memorizzati o trattati in modo continuativo in qualsiasi altro modo), l'interessato deve ricevere accesso e informazioni ai sensi dell'articolo 15 del GDPR.

Limitazioni al diritto di accesso:

- **art. 15 par. 4 del GDPR** (diritto ad ottenere una copia): Dato che un numero qualsiasi di soggetti interessati può essere registrato nella stessa sequenza di videosorveglianza, una proiezione provocherebbe un ulteriore trattamento dei dati personali di altri soggetti. Se l'interessato desidera ricevere una copia del materiale, ciò potrebbe pregiudicare i diritti e le libertà degli altri interessati. Quindi il titolare del trattamento deve attuare misure tecniche per soddisfare la richiesta di accesso.
- **Art. 11, par. 2 del GDPR** (il titolare del trattamento non è in grado di identificare l'interessato): per tali ragioni l'interessato dovrebbe (oltre ad identificarsi anche con documento di identità o di persona) nella sua richiesta al titolare del trattamento, specificare quando - entro un ragionevole lasso di tempo in proporzione alla quantità di dati registrati - è entrato nell'area monitorata.
- **Art. 12, par. 5 del GDPR** (richieste eccessive o manifestamente infondate da parte dell'interessato): in caso di richieste eccessive o manifestamente infondate da parte dell'interessato, il titolare del trattamento può esigere un compenso ragionevole ai sensi dell'articolo 12, paragrafo 5, lettera a), GDPR, oppure rifiutare di dare seguito alla richiesta (articolo 12, paragrafo 5, lettera b), GDPR).

Diritto di cancellazione

Se il titolare del trattamento continua a trattare dati personali al di là del monitoraggio in tempo reale (ad esempio, la conservazione), l'interessato può chiedere la cancellazione dei dati personali ai sensi dell'articolo 17 del GDPR.
Su richiesta, il titolare del trattamento è tenuto a cancellare i dati personali senza indebito ritardo se si verifica una delle circostanze elencate all'articolo 17, paragrafo 1, del GDPR.

Inoltre, a seconda della base giuridica del trattamento, i dati personali devono essere cancellati:

- **per il consenso** ogni volta che il consenso viene ritirato (e non vi sono altre basi legali per il trattamento);
- **per un interesse legittimo**: qualora l'interessato eserciti il diritto di opposizione e non sussistano motivi preminenti e legittimi per opporsi al trattamento, oppure in caso di marketing diretto (inclusa la profilazione) ogni volta che l'interessato si oppone al trattamento.

Diritto di opposizione

Per la videosorveglianza basata su un *interesse legittimo* (articolo 6, paragrafo 1, lettera f), del GDPR) o per la necessità di svolgere un compito di *interesse pubblico* (articolo 6, paragrafo 1, lettera e), del GDPR), l'interessato ha il diritto - in qualsiasi momento - di opporsi, per motivi connessi alla sua situazione particolare, al trattamento ai sensi dell'articolo 21 del GDPR. Naturalmente a meno che il titolare del trattamento non dimostri motivi legittimi e convincenti che prevalgano sui diritti e sugli interessi dell'interessato, il trattamento dei dati deve cessare.

Nel contesto della videosorveglianza l’opposizione dell’interessato potrebbe essere fatta sia all'entrata, sia durante il tempo di permanenza, sia dopo l'uscita dall'area monitorata.
In pratica ciò significa che, a meno che il titolare del trattamento non abbia altri motivi legittimi, il monitoraggio di un'area in cui potrebbero essere identificate persone fisiche è lecito solo se:
(1) il controllore è in grado di interrompere immediatamente il trattamento dei dati personali quando richiesto, oppure
(2) l'area monitorata è limitata in modo così dettagliato che il titolare del trattamento possa assicurare il consenso dell'interessato prima di entrare nell'area e non è un'area alla quale l'interessato, in quanto cittadino, ha diritto di accedere.

Obblighi di trasparenza e di informazione

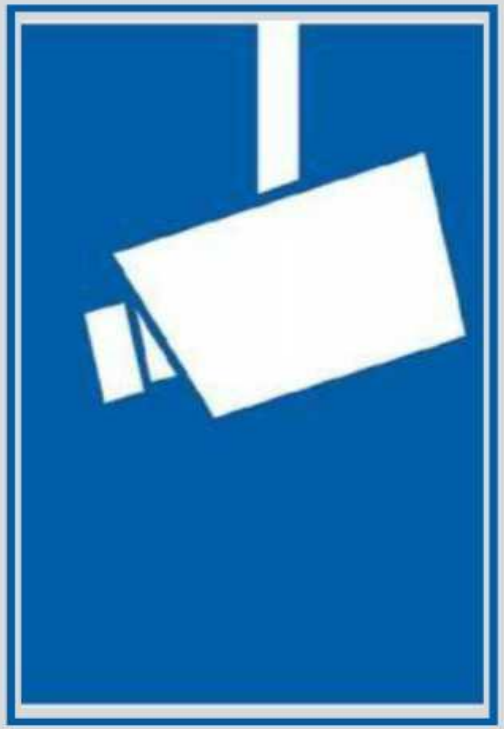
Come noto nell'ambito del GDPR gli obblighi generali di trasparenza e di informazione sono stabiliti dall'articolo 12 GDPR e seguenti. Le "Linee guida sulla trasparenza ai sensi del regolamento 2016/679 (WP260)" del gruppo di lavoro dell'articolo 29, approvate dall'EDPB il 25 maggio 2018, forniscono ulteriori dettagli.
In particolare le linee guida chiariscono che alla luce del volume delle informazioni che devono essere fornite all'interessato, i titolari del trattamento possono seguire un approccio a più livelli, scegliendo di utilizzare una combinazione di metodi per garantire la trasparenza.
Per quanto riguarda la videosorveglianza, le informazioni più importanti dovrebbero essere visualizzate sul cartello stesso (primo livello), mentre gli ulteriori dettagli obbligatori possono essere forniti con altri mezzi (secondo livello).

Informazioni di primo livello

Il primo strato riguarda il modo primario in cui il titolare del trattamento si relaziona per la prima volta con l'interessato. In questa fase, i controllori possono utilizzare un cartello di avvertimento con le relative informazioni.
Le informazioni devono essere posizionate in modo tale che l'interessato possa riconoscere facilmente le circostanze della sorveglianza prima di entrare nell'area monitorata (approssimativamente all'altezza degli occhi).

Le informazioni del primo livello (segnale di avvertimento) dovrebbero essere quelle più importanti, ad esempio i dettagli delle finalità del trattamento, l'identità del titolare del trattamento e l'esistenza dei diritti dell'interessato, insieme alle informazioni sui maggiori impatti del trattamento.
Ciò può includere, ad esempio, gli interessi legittimi perseguiti dal titolare del trattamento (o da un terzo) e i dati di contatto del responsabile della protezione dei dati (se del caso). Deve anche fare riferimento al secondo livello di informazioni più dettagliato e dove e come trovarle.

Esempio:



Identità del Titolare del trattamento:

Dettagli di contatto del Data Protection Officer (DPO/RPD) ove applicabile:

Finalità del trattamento dati personali nonché fonti normative per l'elaborazione:

Diritti dell'interessato: *Sono i diversi diritti dell'interessato al trattamento nei confronti del Titolare, in particolare il diritto di accesso o cancellazione dei dati personali.*

Per tutti i dettagli su questo servizio di videosorveglianza, inclusi i tuoi diritti, consulta le informazioni complete fornite dal Titolare attraverso le opzioni riportate a sinistra.

Informazioni di secondo livello

Le linee guida chiariscono che le informazioni del secondo livello, da fornire nel rispetto dell'art. 13 del GDPR, devono essere messe a disposizione in un luogo facilmente accessibile all'interessato, ad esempio come scheda informativa completa disponibile in una postazione centrale (ad es. sportello informazioni, reception o cassa) o esposta su un poster facilmente accessibile.
Dovrebbe essere possibile accedere alle informazioni del secondo livello senza entrare nell'area censita, soprattutto se le informazioni sono fornite in formato digitale (ciò può essere realizzato ad esempio tramite un link).
Un altro mezzo appropriato potrebbe essere un numero di telefono che può essere chiamato.

Oltre a queste opzioni, l'EDPB promuove l'uso di mezzi tecnologici per fornire informazioni alle persone interessate.
Ciò può includere, ad esempio, la geo-localizzazione delle telecamere e l'inserimento di informazioni nelle applicazioni di mappatura o nei siti web, in modo che gli individui possano facilmente, da un lato, identificare e specificare le fonti video relative all'esercizio dei loro diritti e, dall'altro, ottenere informazioni più dettagliate sull'operazione di elaborazione.

Conservazione ed obbligo di cancellazione

Le linee guida chiariscono che i dati personali non possono essere conservati più a lungo di quanto necessario per le finalità per le quali sono trattati (articolo 5, paragrafo 1, lettere c) ed e) del GDPR). In alcuni Stati membri possono esistere disposizioni specifiche per i periodi di conservazione in materia di videosorveglianza ai sensi dell'articolo 6, paragrafo 2, del GDPR.

In generale, gli scopi legittimi della videosorveglianza sono spesso la protezione della proprietà o la conservazione delle prove. Di solito i danni che si sono verificati possono essere riconosciuti entro uno o due giorni.
Le linee guida evidenziano che per facilitare la dimostrazione del rispetto del quadro normativo sulla protezione dei dati è nell'interesse del titolare del trattamento prendere in anticipo disposizioni organizzative (ad es. nominare, se necessario, un rappresentante per la proiezione e la messa in sicurezza del materiale video).

Tenendo conto dei principi della minimizzazione dei dati e della limitazione della loro conservazione, i dati personali dovrebbero nella maggior parte dei casi (ad esempio per rilevare atti vandalici) essere cancellati, idealmente in modo automatico, dopo pochi giorni.
Quanto più lungo è il periodo di conservazione stabilito (soprattutto se superiore a 72 ore), tanto più si deve argomentare la legittimità dello scopo e la necessità di conservazione.
Se il titolare del trattamento utilizza la videosorveglianza non solo per monitorare i propri locali, ma intende anche memorizzare i dati, deve assicurarsi che la memorizzazione sia effettivamente necessaria.

Il provvedimento generale del Garante

Il provvedimento, ancora valido anche dopo il GDPR, purché compatibile, ha introdotto importanti novità in considerazione:

- dell'aumento massiccio di sistemi di videosorveglianza per diverse finalità (prevenzione, accertamento e repressione dei reati, sicurezza pubblica, tutela della proprietà privata, controllo stradale etc.);
- dei numerosi interventi legislativi adottati in materia: tra questi, quelli più recenti che hanno attribuito ai sindaci e ai comuni specifiche competenze, in particolare in materia di sicurezza urbana, così come le norme, anche regionali, che hanno incentivato l'uso di telecamere.

Principi generali

Il provvedimento del Garante ha dettato dei principi di carattere generale validi sia per i soggetti pubblici che per quelli privati adottati nel rispetto di quelle fondamentali prescrizioni in tema di privacy, di liceità, necessità, proporzionalità e finalità.

Innanzitutto è importante chiarire che l’installazione di telecamere è lecita solo se è proporzionata agli scopi che si intendono perseguire. Gli impianti di videosorveglianza devono essere attivati solo quando altre misure siano insufficienti o inattuabili.

Se è vero che il diritto alla protezione dei dati personali non pregiudica l'adozione di misure efficaci per garantire la sicurezza e l'accertamento degli illeciti è anche vero che l'installazione di sistemi di videosorveglianza non deve però violare la privacy dei cittadini e deve essere conforme al codice in materia di protezione dei dati personali.

La raccolta e l’uso delle immagini sono consentiti solo se fondati su presupposti di liceità: cioè, per i soggetti pubblici, quando siano necessari allo svolgimento di funzioni istituzionali e, per i privati, quando siano necessari per adempiere ad obblighi di legge o effettuate per tutelare un legittimo interesse.

Lo Statuto dei lavoratori

Come è noto, sempre in tema di videosorveglianza, l'art. 23, comma 1, del decreto legislativo n. 151/2015, (attuativo della legge delega n. 183/2014) ha modificato l'art. 4 dello Statuto dei Lavoratori ed in molti hanno pensato ad una vera e propria eliminazione del divieto di controllo a distanza dei lavoratori.

"1. Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo gli impianti e gli strumenti di cui al periodo precedente possono essere installati previa autorizzazione della Direzione territoriale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più Direzioni territoriali del lavoro, del Ministero del lavoro e delle politiche sociali.

2. La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.

3. Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196."

Ma la giurisprudenza della Corte di Cassazione già da un pò di tempo ha iniziato a rivedere l'applicazione dell'art. 4 dello Statuto dei Lavoratori. Difatti, con sentenza n. 4746 del 2002 la Cassazione ha escluso l'applicabilità di detto articolo ai controlli diretti ad accertare condotte illecite del lavoratore, i c.d. controlli difensivi. Il ragionamento della Corte, in tal senso, è chiaro: "Ai fini dell'operatività del divieto di utilizzo di apparecchiature per il controllo a distanza dell'attività dei lavoratori previsto dall'art. 4 l. n. 300 citata, è necessario che il controllo riguardi (direttamente o indirettamente) l'attività lavorativa, mentre devono ritenersi certamente fuori dell'ambito di applicazione della norma i controlli diretti ad accertare condotte illecite del lavoratore (cosiddetti controlli difensivi), quali, ad esempio, i sistemi di controllo dell'accesso ad aree riservate, o gli apparecchi di rilevazione di telefonate ingiustificate.

Successivamente, con la pronuncia n. 15892 del 2007, la Corte ha tuttavia ammesso un limite, affermando che i controlli difensivi non possono giustificare l'annullamento di ogni garanzia: "Né l'insopprimibile esigenza di evitare condotte illecite da parte dei dipendenti può assumere portata tale da giustificare un sostanziale annullamento di ogni forma di garanzia della dignità e riservatezza del lavoratore".

Tale principio è stato riaffermato in numerose pronunce successive e, con la sentenza n. 4375 del 2010, è stato applicato anche ai programmi informatici che consentono il monitoraggio della posta elettronica e degli accessi ad Internet. La sentenza, dopo aver definito tale tipologia di controllo come "controllo preterintenzionale", rientrante perciò nell'ambito di applicazione del secondo comma dell'art. 4 dello Statuto dei lavoratori, ha affermato, quanto segue: "i programmi informatici che consentono il monitoraggio della posta elettronica e degli accessi Internet sono necessariamente apparecchiature di controllo nel momento in cui, in ragione delle loro caratteristiche, consentono al datore di lavoro di controllare a distanza e in via continuativa durante la prestazione, l'attività lavorativa e se la stessa sia svolta in termini di diligenza e di corretto adempimento".

Principali e recenti provvedimenti del Garante

- **Provvedimento n. 100 del 22 febbraio 2024**
- **Provvedimento n. 101 del 22 febbraio 2024**
- **Provvedimento n. 33 del 24 gennaio 2024**
- **Provvedimento n. 612 del 21 dicembre 2023**
- **Provvedimento n. 312 del 18 luglio 2023**