Comunicazione informativa sulla videosorveglianza

Quadro normativo, adempimenti e gestione operativa

1. Oggetto e quadro generale

La videosorveglianza comporta il trattamento di dati personali quando le immagini consentono di identificare, direttamente o indirettamente, una persona fisica. Il trattamento deve quindi rispettare il Regolamento (UE) 2016/679 ("GDPR") e, in particolare, i principi di liceità, correttezza e trasparenza, limitazione della finalità, minimizzazione dei dati, limitazione della conservazione, integrità e riservatezza.

Il "Codice privacy", D.Lgs. n. 101/2018, integra il GDPR e disciplina, tra l'altro, il trattamento dei dati nel rapporto di lavoro e le conseguenze delle violazioni. La valutazione deve rilavare, tra gli altri aspetti, le finalità effettive, le caratteristiche tecniche del sistema, le aree riprese, la presenza di lavoratori, la natura pubblica o privata del titolare e la durata della conservazione.

Per clienti, visitatori, fornitori e altri soggetti esterni, la ripresa destinata alla sicurezza o alla tutela del patrimonio non richiede, di regola, una liberatoria individuale, purché esista un'idonea base giuridica — normalmente riconducibile al legittimo interesse del titolare, salvo diversa valutazione del caso concreto — e siano rispettati necessità, proporzionalità, trasparenza e minimizzazione. Non è normalmente prevista una generale autorizzazione preventiva del Garante né una notificazione ordinaria dell'impianto; restano però necessari gli adempimenti previsti dal GDPR e, per i trattamenti ad alto rischio, la valutazione d'impatto e le eventuali procedure di consultazione preventiva.

2. Presupposti di liceità e rapporto con i lavoratori

L'art. 4 della legge 20 maggio 1970, n. 300 ("Statuto dei lavoratori") stabilisce che, se l'impianto può determinare anche indirettamente un controllo a distanza dell'attività dei lavoratori, esso può essere installato esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro o per la tutela del patrimonio aziendale. In tali casi, prima dell'installazione, è necessario un accordo collettivo con la RSA o la RSU. In mancanza di accordo, occorre una preventiva autorizzazione dell'Ispettorato territoriale del lavoro.

La sola finalità dichiarata di sicurezza non è sufficiente quando, in concreto, il sistema consente di controllare i dipendenti. L'accordo o l'autorizzazione devono precedere l'installazione e la planimetria, il numero delle telecamere, gli angoli di ripresa e le aree interessate devono corrispondere effettivamente al sistema installato. Anche una modifica

non autorizzata della collocazione o del numero delle telecamere può rendere illecito il trattamento.

Il consenso individuale dei dipendenti non sostituisce l'accordo sindacale o l'autorizzazione dell'Ispettorato. La procedura dell'art. 4 tutela infatti un interesse collettivo e non può essere elusa mediante liberatorie o dichiarazioni firmate dai singoli lavoratori. Il consenso può documentare la ricezione di un'informativa, ma non sana la mancanza dei presupposti collettivi o amministrativi.

3. Adempimenti e documentazione

Prima dell'acquisto o dell'attivazione è opportuno predisporre una valutazione preventiva del trattamento. Il titolare dovrebbe documentare le finalità, i rischi, le alternative considerate, il posizionamento e il numero delle telecamere, gli angoli di ripresa, il funzionamento dell'impianto, gli eventuali monitor, DVR, gli orari di funzionamento, i tempi di conservazione, le modalità di accesso e cancellazione, nonché l'eventuale accordo sindacale o autorizzazione amministrativa. La valutazione dovrebbe spiegare perché il sistema sia necessario e proporzionato rispetto al rischio concreto.

La valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35 GDPR deve essere effettuata quando il trattamento presenta un rischio elevato e, in particolare, quando ricorrono monitoraggio sistematico, sorveglianza su larga scala di aree accessibili al pubblico, uso di sistemi intelligenti, registrazione audio, riconoscimento facciale o altre funzioni automatizzate. La **Valutazione d'impatto sulla protezione dei dati** (DPIA) deve essere svolta prima dell'avvio del trattamento e deve considerare anche le misure adottate per ridurre i rischi. La soglia e le modalità di applicazione dipendono comunque dalle caratteristiche effettive dell'impianto.

Il sistema dovrebbe essere inserito nel registro dei trattamenti del titolare, con indicazione delle finalità, delle categorie di interessati e di dati, dei destinatari, dei tempi o criteri di cancellazione e delle misure di sicurezza. Il principio di accountability impone non solo di rispettare la normativa, ma anche di poter dimostrare la conformità delle scelte compiute.

La società che installa, gestisce, conserva o visiona le immagini per conto dell'azienda deve essere qualificata, ove ne ricorrano i presupposti, come responsabile del trattamento ai sensi dell'art. 28 GDPR. Il rapporto deve essere regolato da un contratto scritto contenente istruzioni, limiti di accesso, misure di sicurezza, disciplina della subfornitura, modalità di cancellazione e restituzione dei dati. La mancata nomina tempestiva del responsabile ha già determinato interventi sanzionatori del Garante.

4. Installazione e gestione operativa

Le finalità devono essere definite in modo specifico, ad esempio con riferimento alla prevenzione di furti, danneggiamenti, accessi non autorizzati, rischi per la sicurezza dei lavoratori o tutela di aree sensibili. Non sono invece adeguate finalità generiche o formule come "controllo dell'attività del personale". Prima di scegliere la videosorveglianza devono essere verificate le alternative meno invasive, quali allarmi, controllo degli accessi, illuminazione, blindature o altri sistemi di sicurezza fisica. L'impianto deve risultare realmente necessario e proporzionato al rischio.

La progettazione deve seguire i principi di minimizzazione e di privacy by design. L'angolo visuale va limitato alle aree da proteggere, evitando per quanto possibile postazioni di lavoro, badge, tastiere, spogliatoi, bagni e luoghi riservati. Salvo necessità documentata, devono essere disattivati audio, zoom automatico, riconoscimento facciale e funzioni analitiche. Devono inoltre essere evitate riprese eccedenti di strade, edifici, proprietà o aree di terzi.

L'accordo sindacale o l'autorizzazione ITL, quando ricorra la possibilità di controllo a distanza, devono essere ottenuti prima dell'installazione. Ogni successiva variazione dell'impianto dovrebbe essere verificata rispetto alla documentazione autorizzativa e alla valutazione privacy, perché una modifica sostanziale può richiedere un aggiornamento dell'accordo, dell'autorizzazione, della DPIA o dell'informativa.

Il sistema deve essere accompagnato da procedure interne per la visione, l'estrazione, la comunicazione e la cancellazione dei filmati, nonché da lettere di designazione degli autorizzati al trattamento, istruzioni operative, un regolamento interno sull'uso dell'impianto e attestazioni di formazione.

5. Informativa, conservazione e sicurezza

L'informativa deve essere predisposta su più livelli. Prima dell'ingresso nell'area sorvegliata devono essere collocati cartelli visibili e facilmente riconoscibili, contenenti almeno l'identità del titolare e le finalità essenziali. Deve inoltre essere disponibile un'informativa di secondo livello, facilmente accessibile presso la reception, sul sito aziendale o tramite altro canale individuabile, con tutti gli elementi dell'art. 13 GDPR: base giuridica, categorie di dati, destinatari, tempi o criteri di conservazione, diritti degli interessati, contatti del titolare e dell'eventuale DPO, modalità di esercizio dei diritti e indicazione di eventuali trasferimenti extra UE.

Il periodo di conservazione deve essere stabilito e motivato in relazione a finalità, rischio e contesto. Non esiste un termine uniforme e automatico valido per ogni impresa. Nella maggior parte dei casi le immagini dovrebbero essere cancellate dopo pochi giorni; un periodo superiore a 72 ore richiede una motivazione particolarmente accurata, senza che

tale soglia costituisca un limite rigido o una regola sostitutiva della valutazione concreta. Le immagini relative a un evento illecito possono essere isolate e conservate più a lungo, per il tempo necessario alla denuncia, alla difesa in giudizio o alla richiesta dell'autorità.

Gli accessi devono essere regolati mediante credenziali individuali, profili differenziati, autenticazione forte, divieto di accessi generalizzati, registrazione dei log, procedure per l'estrazione dei filmati e formazione degli autorizzati. Il D.P.R. 15 gennaio 2018, n. 15 prevede, per gli specifici trattamenti cui si applica, livelli differenziati di visibilità, protezione contro accessi abusivi e conservazione dei log per cinque anni. L'applicazione di tali prescrizioni deve essere verificata rispetto all'ambito soggettivo e oggettivo del singolo trattamento.

I dipendenti devono essere informati sulle modalità d'uso degli strumenti e sulle modalità di effettuazione dei controlli. L'art. 4, comma 3, dello Statuto dei lavoratori consente l'utilizzo delle informazioni raccolte anche per fini connessi al rapporto di lavoro solo quando il lavoratore sia stato adeguatamente informato e sia stata rispettata la disciplina sulla protezione dei dati.

6. Dipendenti, clienti, visitatori e fornitori

Per i dipendenti è opportuno predisporre una dichiarazione di avvenuta consegna e presa visione dell'informativa, nella quale siano indicati o richiamati l'identità e i contatti del titolare, le finalità e la base giuridica, le aree riprese e le modalità di funzionamento, l'eventuale registrazione audio o accesso da remoto, i tempi di conservazione, i soggetti autorizzati alla visione, l'eventuale comunicazione alle autorità, i diritti dell'interessato e le modalità di esercizio, nonché le condizioni di utilizzabilità delle immagini per fini connessi al rapporto di lavoro.

La firma ha una funzione documentale e probatoria della consegna dell'informativa: non costituisce consenso e non sana l'eventuale mancanza dell'accordo sindacale o dell'autorizzazione ITL. L'informativa deve essere fornita prima dell'inizio del trattamento. La documentazione interna dovrebbe inoltre comprendere le designazioni degli autorizzati, le istruzioni operative, il regolamento, la formazione e, quando pertinente, l'informativa integrativa sugli strumenti automatizzati prevista dall'art. 1-bis del D.Lgs. n. 152/1997.

Per clienti, visitatori e fornitori è normalmente sufficiente una cartellonistica conforme, accompagnata da un'informativa completa accessibile presso la reception, sul sito aziendale o mediante altro canale facilmente individuabile. La "liberatoria" non dovrebbe essere utilizzata come sostituto dell'informativa né come consenso generalizzato alla videosorveglianza.

Un consenso specifico può diventare rilevante per finalità ulteriori e distinte rispetto alla sicurezza o alla tutela del patrimonio, come la pubblicazione delle immagini sul sito o sui social, l'uso promozionale o pubblicitario, la diffusione di immagini riconoscibili, riprese audio o video non necessarie alla sicurezza oppure, ove astrattamente consentito dalla normativa applicabile, il trattamento biometrico o il riconoscimento facciale. Le immagini dei clienti non possono essere utilizzate per finalità diverse da quelle dichiarate senza un'ulteriore base giuridica e un'adeguata informativa.

7. Sanzioni, utilizzabilità delle immagini e conseguenze

Per violazioni degli obblighi informativi, dei principi di liceità, minimizzazione, conservazione e sicurezza, degli obblighi relativi alla DPIA o dei diritti degli interessati, il GDPR prevede, in funzione della violazione, sanzioni fino a 20 milioni di euro oppure al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore. Il Garante può inoltre adottare provvedimenti correttivi, tra cui l'ordine di adeguamento, la limitazione o il divieto del trattamento e la cancellazione dei dati.

Tra i casi sanzionatori richiamati figurano un provvedimento da 20.000 euro nei confronti di un'azienda che utilizzava videosorveglianza con audio e accesso da smartphone, in assenza di cartelli e di accordo sindacale o autorizzazione dell'Ispettorato, nonché un provvedimento da 10.000 euro relativo a un impianto modificato rispetto all'accordo sindacale e attivato senza adeguata informativa e DPIA.

L'installazione di impianti audiovisivi in violazione dell'art. 4 dello Statuto dei lavoratori può integrare il reato previsto dall'art. 171 del Codice privacy, in relazione all'art. 38 dello Statuto, con arresto fino a un anno e/o ammenda, secondo la disciplina applicabile. La responsabilità può derivare anche dalla mera installazione di un impianto potenzialmente idoneo al controllo, senza che sia necessario dimostrare l'effettivo utilizzo delle immagini.

Quando le immagini siano acquisite in violazione della disciplina privacy o dell'art. 4 dello Statuto, esse possono risultare inutilizzabili in sede disciplinare o lavoristica. La giurisprudenza richiamata ha escluso l'utilizzabilità di dati acquisiti illegittimamente quando il datore non dimostri il rispetto delle regole applicabili. Se un provvedimento disciplinare si fonda su immagini inutilizzabili, il licenziamento o altra sanzione possono essere dichiarati illegittimi.

I controlli difensivi "in senso stretto", diretti ad accertare specifici illeciti sulla base di un fondato sospetto, possono essere valutati diversamente rispetto ai controlli ordinari sull'attività lavorativa. Anche in tale ipotesi, tuttavia, devono essere proporzionati e rispettare la normativa generale sulla protezione dei dati, oltre alle ulteriori garanzie eventualmente applicabili.

Il trattamento illecito può esporre l'azienda a reclami al Garante, richieste di accesso e cancellazione, contenzioso sindacale, impugnazioni disciplinari e domande risarcitorie per danni patrimoniali o non patrimoniali, oltre alle eventuali responsabilità amministrative e penali.

8. Conclusione operativa

La procedura più prudente consiste nel predisporre, prima dell'acquisto o dell'attivazione, un progetto tecnico e una valutazione di necessità e proporzionalità; verificare le alternative meno invasive; ottenere l'accordo sindacale o l'autorizzazione ITL quando ricorra la possibilità di controllo a distanza; svolgere, se necessaria, la DPIA; aggiornare il registro dei trattamenti; disciplinare il rapporto con i fornitori; predisporre cartelli di primo livello e informativa completa; adottare autorizzazioni interne, policy di accesso, procedure di estrazione e cancellazione e misure di formazione.

Le firme dei dipendenti documentano la ricezione dell'informativa, ma non sostituiscono gli adempimenti collettivi e amministrativi previsti dall'art. 4 dello Statuto dei lavoratori. La decisione finale deve essere verificata alla luce delle caratteristiche concrete dell'impianto, delle aree riprese, della presenza di lavoratori, delle finalità perseguite, dei tempi di conservazione e della natura del titolare.