Sempre più forte la convergenza tra Safety e Security nel contesto normativo italiano in materia di videosorveglianza nei luoghi di lavoro

Anna Villani
Project Manager & BDM | Presidente Vicario APC Security & Safety AIAS Sicurezza| Security Manager Certificato UNI 10459
in

Con sempre maggiore forza, il contesto normativo italiano mette in luce la necessità per le imprese di dotarsi di un modello di analisi dei rischi basato sulla **convergenza tra Safety e Security**, come ben ci illustrano gli orientamenti giurisprudenziali e le sentenze della Corte di Cassazione in applicazione del Decreto Legislativo n. 81/08 (Testo Unico sulla Salute e Sicurezza dei Lavoratori) e del Decreto Legislativo n. 231/01 (Responsabilità Amministrativa degli Enti), che obbligano il datore di lavoro a valutare come connessi all'attività lavorativa non solo i "*rischi tipici*" della materia antinfortunistica, ma anche i cosiddetti "rischi atipici" che possono scaturire dalle attività di origine criminosa.

La rilevanza giuridica di un modello di "**Safety & Security Risk Assessment**" a supporto della compliance normativa per le organizzazioni aziendali entra ora pieno regime anche nell'articolato e complesso mondo delle leggi e dei provvedimenti applicati alla videosorveglianza sui luoghi di lavoro, come ci dimostrano gli importanti chiarimenti interpretativi emanati lo scorso anno **dall'Ispettorato Nazionale del Lavoro** e dal **Garante della Privacy** italiano, e che andremo di seguito ad approfondire.

Fig. 1 – Risk Assessment e convergenza Safety & Security

Fig. 2 – Videosorveglianza e Compliance normativa

Ispettorato Nazionale del Lavoro

Nel corso del 2018, l'Ispettorato Nazionale del Lavoro (INL) ha emanato due importanti circolari indirizzate alle sedi territoriali in materia di verifica ispettiva ed autorizzativa inerenti la videosorveglianza, ai sensi dell'**art. 4 dello Statuto dei Lavoratori** (Legge n. 300/1970) e sue successive modifiche.

Con la Circolare n. 5 del 19 febbraio 2018, l'INL specifica come l'attività di controllo ispettivo debba verificare la "*effettiva sussistenza delle ragioni legittimanti l'adozione del provvedimento*" e che le modalità di utilizzo degli strumenti di controllo "*siano assolutamente conformi e coerenti con le finalità dichiarate*". L'INL chiarisce inoltre come tali ragioni alla base del consenso autorizzativo non possano essere assolutamente di "*carattere generico*", ma corrispondano ad effettive "*ragioni di sicurezza sul lavoro* (**Safety**)", e/o "*ragioni di protezione del patrimonio*" (**Security**), debitamente "*comprovate*", ovvero risultino essere una misura necessaria di mitigazione di tali rischi, opportunamente documentata.

Tale principio viene ulteriormente confermato dall'INL attraverso la circolare n. 302 del 18 giugno 2018 che fornisce alle sedi territoriali ulteriori indicazioni operative da applicare in fase autorizzativa, "*qualora le istanze presentate siano legate ad esigenze di sicurezza del lavoro*".

La circolare n. 302/2018 specifica, inoltre, come le addotte ragioni di sicurezza sul lavoro debbano trovare "*adeguato riscontro nell'attività di valutazione dei rischi effettuata dal datore di lavoro e formalizzata nell'apposito documento (DVR)*" e che l'istanza autorizzativa debba necessariamente "*essere corredata dagli estratti del documento di valutazione dei rischi*".

GDPR

Come abbiamo anticipato, la conduzione di una preventiva analisi di rischio in materia di videosorveglianza sui luoghi di lavoro è divenuta un elemento fondamentale di compliance normativa anche in ai sensi del **GDPR**[1] .

Con il Provvedimento n. 467 dell'11 ottobre 2018, il **Garante della Privacy** italiano, difatti, ha incluso l'attività di controllo a distanza dei lavoratori dipendenti tramite sistemi di **videosorveglianza sul luogo di lavoro** tra le "*tipologie dei trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto (DPIA)*", ai sensi dell'art. 35 del GDPR.

La **DPIA**, letteralmente **Data Protection Impact Assessment**, consiste in una procedura finalizzata a descrivere la valutazione di impatto di un trattamento, valutandone **necessità** e **proporzionalità**, e facilitare la gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei loro dati personali.

La DPIA è uno strumento importante in termini di responsabilizzazione (accountability) in quanto aiuta il titolare non soltanto a rispettare le prescrizioni del GDPR, ma anche a "*dimostrare l'adozione di misure idonee a garantire il rispetto di tali prescrizioni.*"

In altri termini, la DPIA è una procedura che permette di realizzare e dimostrare la conformità con le norme e in base al regolamento. L'inosservanza degli obblighi concernenti la DPIA può comportare l'imposizione di pesanti sanzioni pecuniarie da parte della competente autorità di controllo.

Il mancato svolgimento della DPIA quando il trattamento è soggetto a tale valutazione, lo svolgimento non corretto di una DPIA o la mancata consultazione dell'autorità di controllo competente

1 General Data Protection Regulation in riferimento al regolamento (UE) n. 2016/679

ove ciò sia necessario (artt. 35 e 36 del GDPR), difatti, possono comportare l'irrogazione di una sanzione amministrativa pecuniaria fino a un massimo di 10 milioni di euro, ovvero, se si tratta di un'impresa, fino al 2% del fatturato mondiale totale annuo dell'esercizio finanziario precedente, se superiore.

Il collegamento diretto tra la DPIA e la preventiva analisi dei rischi in capo all'impresa ci viene ben spiegato da una nota illustrativa del Garante della Privacy stesso, che la descrive come una "*procedura che mira a descrivere un trattamento di dati per valutarne l'effettiva* ***necessità*** *e* ***proporzionalità***".

Secondo il principio della responsabilizzazione o "*accountability*", ai sensi dell'art. 5 del GDPR, i titolari debbono poi "***essere in grado di comprovarlo***".

In materia di **videosorveglianza**, pertanto, il titolare deve dimostrare nell'elaborazione della DPIA, di aver eseguito, precedentemente al trattamento, la valutazione dei rischi dai quali ne risulti la legittimità quale misura mitigativa necessaria, proporzionale e prevalente sui diritti e sulle libertà fondamentali dei lavoratori interessati.

Deve inoltre dimostrare di aver correttamente applicato i seguenti principi cardine del nuovo regolamento:

- liceità, correttezza e trasparenza
- limitazione e rispetto della finalità
- minimizzazione, necessità e pertinenza
- esattezza e aggiornamento, compresa la tempestiva cancellazione dei dati che risultino inesatti
- limitazione della conservazione, per un tempo non superiore a quello necessario rispetto agli scopi
- integrità e riservatezza, ovvero garantirne l'adeguata sicurezza.

Per lo svolgimento della DPIA, infine, è opportuno tenere conto delle linee-guida in materia di valutazione di impatto sulla protezione dei dati elaborate del Gruppo "Articolo 29" (WP 29), ovvero dall'organo consultivo indipendente dell'UE per la protezione dei dati personali che, nel seguente schema illustrativo del processo, ben illustra come necessarie le fasi di:

- valutazione della necessità e proporzionalità del trattamento, in cui la legittimità risulti essere prevalente sui diritti e sulle libertà fondamentali dell'interessato
- Predisposizione della documentazione necessaria a comprovarlo.

L'interesse legittimante del titolare ad installare e utilizzare sistemi di videosorveglianza sui luoghi di lavoro dovrà, pertanto, risultare quale misura di mitigazione necessaria e proporzionale debitamente dimostrata da una preventiva attività di *Risk Assessment* convergente tra rischi di *Safety e Security*, in grado di comprovare quelle "effettive ragioni" di sicurezza del patrimonio e tutela dei lavoratori che ne sono alla base. ■

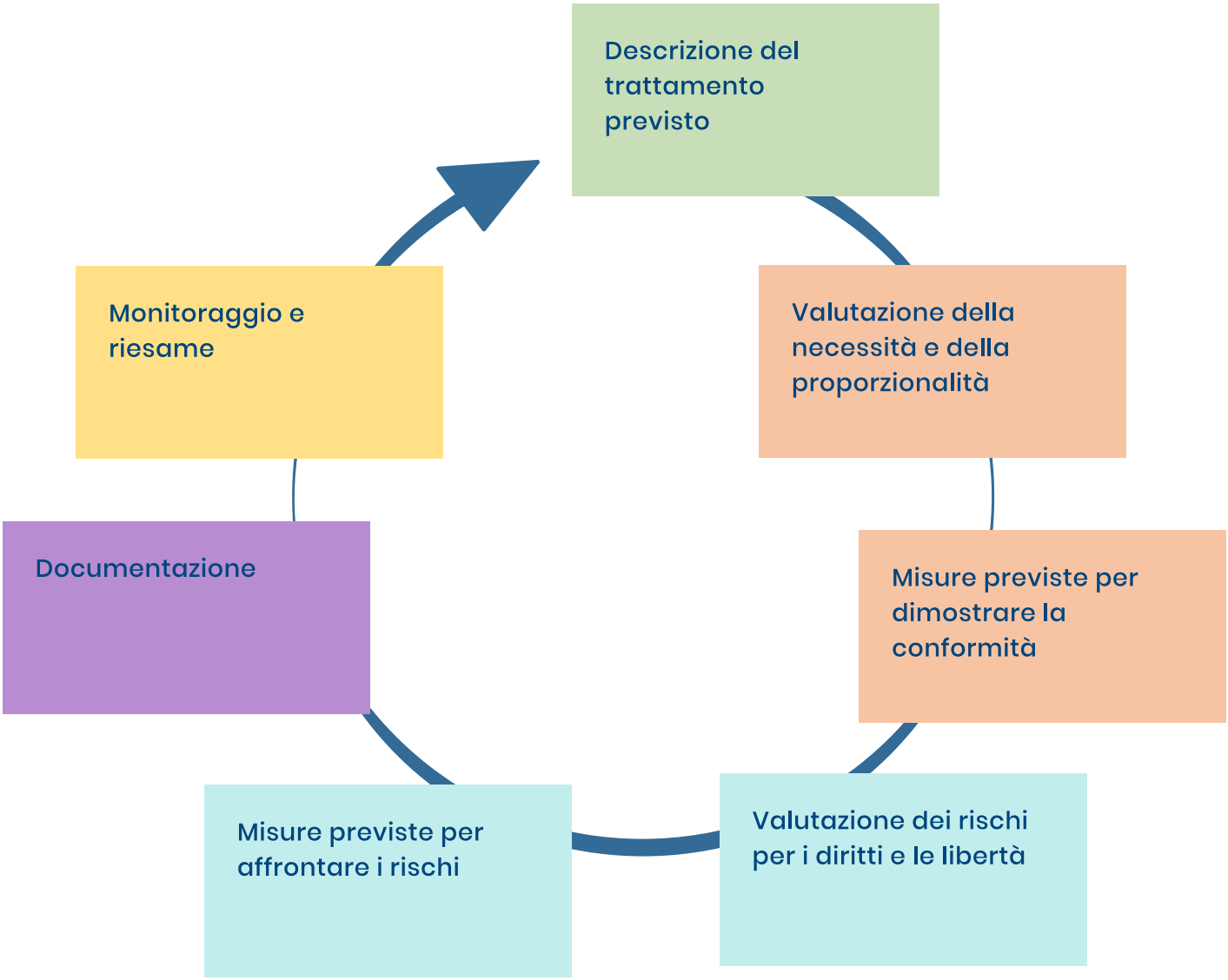

Fig. 2 - Linee-guida DPIA WK 29