ASSOLOMBARDA

La Privacy nel controllo a distanza

Dispensa n°04/2022

A cura
Settore Fisco e Diritto d'Impresa

La dispensa è stata chiusa in data 10 dicembre 2021

Indice Contenuti

1

Premessa

Per rispondere al mutato contesto tecnologico, il Legislatore ha modificato l'art. 4 dello Statuto dei Lavoratori con l'art. 23 del Decreto Legislativo 14 settembre 2015, n. 151 (c.d. decreto semplificazioni) nell'ambito della riforma del mercato del lavoro denominato «Jobs Act», in attuazione della legge delega n. 183 del 2015 conferita al governo di revisione della disciplina dei controlli a distanza sugli impianti e sugli strumenti di lavoro.

La nuova normativa riprende il principio generale espresso nell'articolo 4 della legge n. 300/1970, con poche modifiche.

Secondo il comma 1 dell'art. 4: "*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.*"

Se l'azienda non raggiunge un accordo a livello sindacale o non ha presenti rappresentanze sindacali, può presentare richiesta di autorizzazione all'installazione degli strumenti alla sede territoriale dell'Ispettorato nazionale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali, alla sede centrale dell'Ispettorato nazionale del lavoro.

Il comma 2 dell'articolo 4 ci dice che non è richiesto l'accordo sindacale o l'autorizzazione all'ispettorato, secondo le regole sopra descritte, in caso di strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e di strumenti di registrazione degli accessi e delle presenze (es. badge).

È doveroso sottolineare che va comunque sempre verificato se l'impianto o lo strumento di lavoro che si vuole utilizzare, potendo essere nel caso concreto anche indirettamente un mezzo di controllo a distanza, richieda la preventiva stipula di un accordo sindacale o di un'autorizzazione in base ai limiti imposti dalla legge e precedentemente descritti.

L'azienda, quindi, oltre a dover gestire il tema della privacy affrontato nella dispensa, deve verificare il rispetto dei requisiti/limiti previsti dalla legge - dal punto di vista giuslavoristico - per l'installazione di impianti/strumenti dai quali può derivare un controllo a distanza secondo quanto previsto nei commi 1 e 2 dell'articolo 4 della legge 300 del 1970.

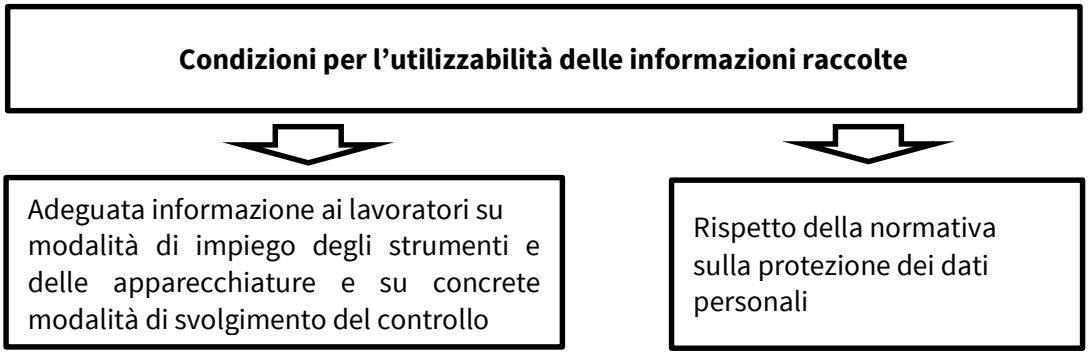
La dispensa - senza entrare nel merito dei suddetti aspetti giuslavoristici - vuole approfondire il tema del controllo a distanza esclusivamente da punto di vista della privacy trattato nel comma 3 dell'articolo 4 che prevede come **"***Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili 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."*

2

L’obbligo di rispettare la normativa sulla protezione dei dati personali

Per regolamentare i limiti e le modalità dell’utilizzo da parte del datore di lavoro dei dati legittimamente raccolti ai sensi dei commi 1 e 2 dell’art. 4 dello Statuto dei Lavoratori, il Legislatore ha rinviato alle norme che regolamentano il trattamento dei dati personali costituito dal Codice in materia di protezione dei dati personali che è stato rivisto e modificato ad opera del Decreto Legislativo n. 101 del 2018, per adeguarlo alla normativa comunitaria di cui al nuovo Regolamento UE 2016/679.

In altri termini, i dati raccolti dagli strumenti in questione **devono essere trattati nel rispetto dei principi fondamentali prescritti dal Regolamento UE 2016/679**, altrimenti il loro utilizzo è illegittimo.



3

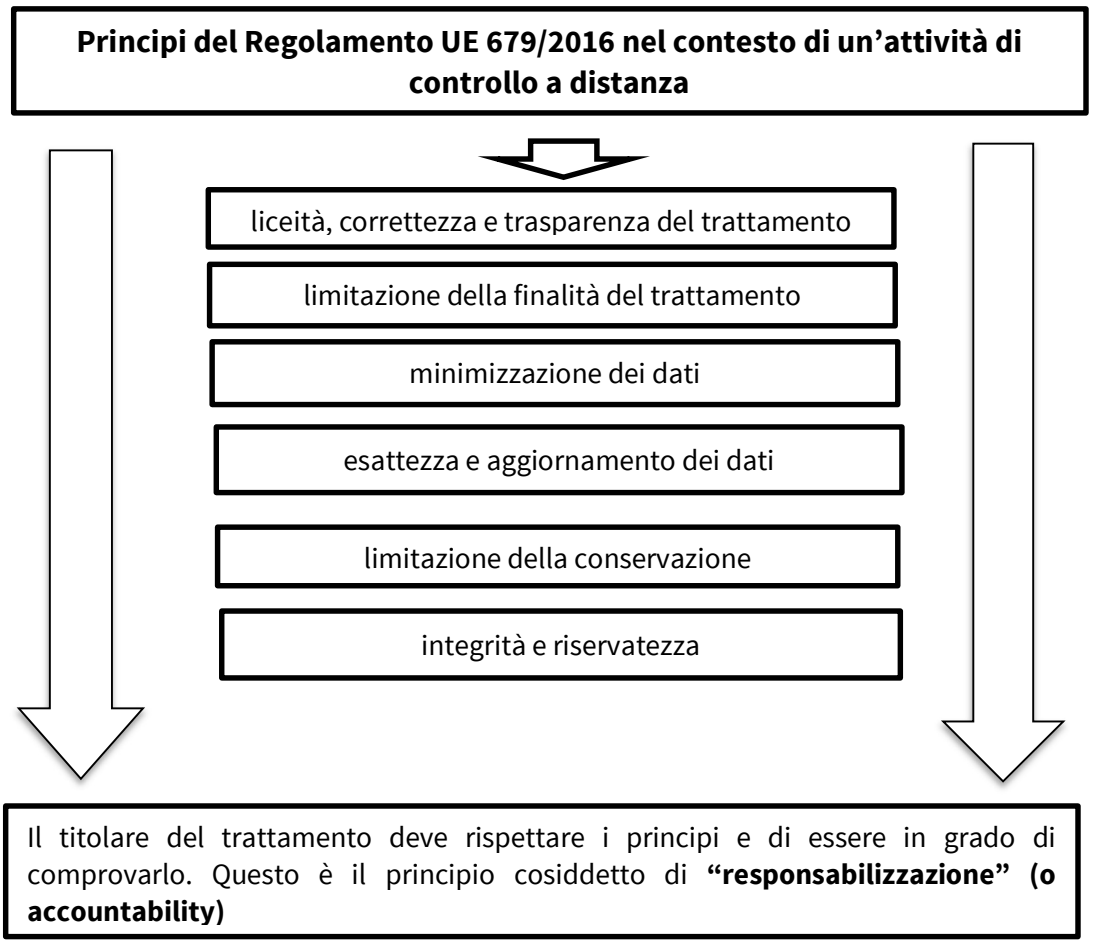
I principi del Regolamento UE 679/2016

In materia di protezione dei dati personali, per interpretare correttamente quanto enunciato dall'art. 4 dello Statuto dei Lavoratori, è indispensabile richiamare alcuni dei principi fissati dall'articolo 5 del Regolamento UE di seguito riportati:

- **liceità, correttezza e trasparenza del trattamento**, nei confronti dell'interessato;
- **limitazione della finalità del trattamento**, compreso l'obbligo di assicurare che eventuali trattamenti successivi non siano incompatibili con la finalità iniziale della raccolta dei dati;
- **minimizzazione dei dati**, ossia i dati devono essere adeguati e limitati a quanto necessario rispetto alle finalità del trattamento;
- **esattezza e aggiornamento dei dati**, compresa la tempestiva cancellazione dei dati che risultino inesatti rispetto alle finalità del trattamento;
- **limitazione della conservazione**, ossia necessità di procedere alla conservazione dei dati per un tempo non superiore a quello necessario rispetto agli scopi per i quali è stato effettuato il trattamento;
- **integrità e riservatezza**, ossia garantire la sicurezza adeguata dei dati personali oggetto del trattamento.

Il Regolamento (art. 5, paragrafo 5) richiede al titolare di rispettare tutti questi principi e di essere in grado di comprovarlo. Questo è il principio cosiddetto di **"responsabilizzazione" (o accountability),** che viene poi esplicitato ulteriormente dall'art. 24, paragrafo 1, del Regolamento, dove si afferma che *"il titolare mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente Regolamento".*

In ogni caso, l'applicazione dei principi fondamentali del Regolamento al contesto dell'articolo 4 dello Statuto dei lavoratori impone al datore di lavoro che abbia accidentalmente raccolto informazioni ulteriori rispetto a quelle relative alla finalità dichiarata, soprattutto se di natura "particolare" o "sensibile" (quali quelle concernenti la salute, le opinioni politiche, sindacali o religiose) o sull'attività lavorativa e, comunque, non pertinenti rispetto alla finalità originaria della raccolta, di procedere alla loro cancellazione, nel rispetto del principio di "minimizzazione" dei dati.



4

L’informativa privacy nel controllo a distanza

Anche nell’ambito del controllo a distanza spetta al datore di lavoro l’obbligo di fornire al lavoratore **un’informativa conforme alle prescrizioni dell’art. 13 del GDPR**, declinata con riferimento a tutte le operazioni di trattamento dei dati poste in essere. Questa rappresenta un adempimento irrinunciabile al quale il titolare del trattamento deve sempre attenersi e il cui contenuto minimo comprende:

- l’identità e dati di contatto del Titolare del trattamento:
- i dati di contatto del Responsabile per la Protezione dei dati o DPO, ove nominato;
- le finalità del trattamento;
- la base giuridica del trattamento;
- l’indicazione dei legittimi interessi del titolare, qualora il trattamento trovi fondamento nei medesimi;
- gli eventuali destinatari dei dati personali;
- il termine di conservazione dei dati personali;
- l’intenzione, ove applicabile, di trasferire i dati in un Paese terzo rispetto alla UE;
- l’esercizio dei diritti dell’interessato.

Informativa art. 13 Regolamento UE 679/2016

Identità e dati di contatto del Titolare del trattamento

Dati di contatto del Responsabile per la Protezione dei dati o DPO, ove nominato

Base giuridica del trattamento

Eventuali destinatari dei dati personali

Termine di conservazione dei dati personali

Intenzione, ove applicabile, di trasferire i dati in un Paese terzo rispetto alla UE

Esercizio dei diritti dell'interessato

5

La videosorveglianza

Le strumentazioni tecnologiche che consentono al datore di lavoro di trattare dati personali dei propri dipendenti e collaboratori costituiscono un fattore di rischio per la riservatezza di quest'ultimi, che l'ordinamento intende tutelare attraverso la prescrizione di limitazioni e accorgimenti. Si ricorda che, dal punto di vista giuslavoristico, l'azienda prima di installare un sistema di videosorveglianza dal quale può derivare un controllo a distanza dei lavoratori deve sempre verificare l'esistenza delle esigenze aziendali individuate nell'articolo 4 della Legge 300 del 1970 e seguire le relative procedure in esso indicate.

Un sistema di videosorveglianza è costituito da dispositivi analogici e digitali e da un software che permette di catturare le immagini di una scena, gestirle e mostrarle all'operatore preposto (es. il titolare del trattamento o un suo dipendente). I suoi componenti sono raggruppati nelle seguenti categorie:

- ambiente video (acquisizione delle immagini, interconnessioni e gestione delle immagini). Lo scopo della cattura delle immagini è la generazione di un'immagine del mondo reale in un formato tale da poter essere utilizzata dal sistema di videosorveglianza. Le interconnessioni descrivono tutte le trasmissioni di dati all'interno dell'ambiente video (connessioni e comunicazioni). Esempi di connessioni sono i cavi, le connessioni digitali e le trasmissioni wireless. Le comunicazioni descrivono tutti i segnali video e di controllo dei dati, che possono essere digitali o analogici. La gestione delle immagini include l'analisi, la

memorizzazione e la presentazione di un'immagine o di una sequenza di immagini;
- data management e activity management, che comprendono la gestione dei comandi dell'operatore e delle attività generate dal sistema (procedure di allarme, avviso degli operatori);
- le interfacce con altri sistemi possono includere il collegamento con altri relativi alla sicurezza (controllo accessi, allarme antincendio) e con altri che non riguardano la sicurezza (sistemi di gestione degli edifici, riconoscimento automatico delle targhe).

Il controllo operato attraverso sistemi di videosorveglianza è una pratica molto diffusa negli ambienti di lavoro. Negli ultimi anni i sistemi di monitoraggio video sono notevolmente cambiati, principalmente con riferimento alla riduzione delle dimensioni delle telecamere, associata ad un aumento della capacità di definizione delle immagini, alla possibilità di accedere facilmente a distanza ai dati raccolti tramite smartphone, all'implementazione di tecniche di analisi delle immagini e della c.d. **"videosorveglianza intelligente"** (sono in commercio numerose soluzioni di analisi video che permettono, ad esempio, l'attivazione di funzioni di *motion detection e motion tracking* o il rilevamento delle espressioni facciali, al fine di individuare deviazioni da modelli di movimento predefiniti).
L'utilizzo delle descritte tecnologie sul posto di lavoro complica, rispetto ai sistemi "classici" di videosorveglianza, il quadro di valutazione della compliance allo Statuto dei lavoratori, per il divieto di installazione di apparecchiature preordinate al controllo (ai sensi dell'art. 4, comma 1, dello Statuto dei Lavoratori), nonché ai fini della normativa privacy (considerata la pervasività di tali sistemi nella sfera di riservatezza del lavoratore).

Il trattamento delle immagini dei lavoratori basato su un sistema di monitoraggio video potrebbe essere realizzato solo ed esclusivamente in presenza delle **esigenze organizzative o produttive**, ovvero di sicurezza del lavoro previste dalla legge, e comunque **nel rigoroso rispetto delle garanzie poste a presidio dei diritti e delle libertà del lavoratore.**

Indicazioni circa la conformità del trattamento delle immagini alla normativa in materia di protezione dei dati personali si rinvengono con le *"Linee Guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video"*, elaborate dal Comitato europeo per la protezione dei dati (Edpb).

Cos'è un sistema di videosorveglianza?

È costituito da dispositivi analogici e digitali e da un software che permette di catturare le immagini di una scena, gestirle e mostrarle all'operatore preposto (il titolare del trattamento)

5.1 IL LEGITTIMO INTERESSE

Nelle sopracitate linee guida Edpb è evidenziato come la base giuridica utile per l'elaborazione dei dati di videosorveglianza risieda nel **legittimo interesse** (art. 6, par. 1, lett. f del GDPR) o nella **necessità di procedere al trattamento di dati da parte di autorità pubbliche nell'esecuzione dei loro compiti** (art. 6, par. 1, lett. e del GDPR).

Qualora il lavoratore interessato si opponga alla videosorveglianza, il titolare del trattamento potrà effettuarla soltanto qualora **l'interesse legittimo sia prevalente rispetto agli interessi, ai diritti e le libertà dell'interessato** o per l'istituzione, l'esercizio o la difesa di rivendicazioni legali. L'esistenza del legittimo interesse deve essere verificata rispetto all'attualità e all'entità della problematica che rende necessario avviare la videosorveglianza nei luoghi di lavoro. Infatti, **nelle linee guida il Comitato europeo per la protezione dei dati ribadisce che il legittimo interesse deve esistere realmente e deve rappresentare una problematica attuale** (cioè non deve essere immaginario o speculativo). In via esemplificativa, riferendosi a situazioni reali di pericolo, di protezione della proprietà da furto o vandalismo, l'Epdb precisa che prima di iniziare la videosorveglianza, alla luce del principio di responsabilità, i titolari del trattamento sarebbero invitati a documentare gli incidenti rilevanti (data, modalità, perdita finanziaria). Tali incidenti documentati possono essere una prova evidente dell'esistenza di un interesse legittimo. Una situazione di pericolo imminente può essere presunta e, dunque, costituire un interesse legittimo nel caso di negozi preposti alla vendita di beni preziosi (ad esempio gioielli) o attività esposte al rischio di crimini contro la proprietà (ad esempio le stazioni di benzina).

In ossequio ai principi di legittimità e determinatezza del fine perseguito, nonché di proporzionalità, correttezza e non eccedenza del trattamento**, si impone al titolare del trattamento di rendere residuali i controlli più invasivi**, **legittimandoli solo a fronte di rilevazione di specifiche anomalie.** Ciò rileva soprattutto per l'utilizzo delle nuove tecnologie di videosorveglianza. **Secondo il principio di necessità**, inoltre, i dati personali trattati devono essere adeguati, pertinenti e limitati a quanto necessario in relazione alle finalità per i quali vengono elaborati ("minimizzazione dei dati"). Quindi**, l'installazione di un sistema di videosorveglianza deve essere sempre preceduta da un esame critico atto a verificare che le misure di controllo adottate siano adatte al raggiungimento dell'obiettivo desiderato nonché adeguate e necessarie ai suoi scopi.**

Inoltre, il controllo a distanza tramite la videosorveglianza **dovrebbe essere scelto solo qualora lo scopo del trattamento non possa ragionevolmente essere raggiunto da altri mezzi meno invasivi dei diritti e delle libertà fondamentali dell'interessato**.

La base giuridica della videosorveglianza

Il legittimo interesse, a condizione che prevalga sugli interessi, i diritti e le libertà delle persone interessate

5.2 IL TEMPO DI CONSERVAZIONE

In applicazione del principio di proporzionalità, nei casi in cui sia stato scelto un sistema che preveda la **conservazione delle immagini**, questa deve essere temporanea e commisurata al tempo necessario e predeterminato a raggiungere la finalità perseguita.

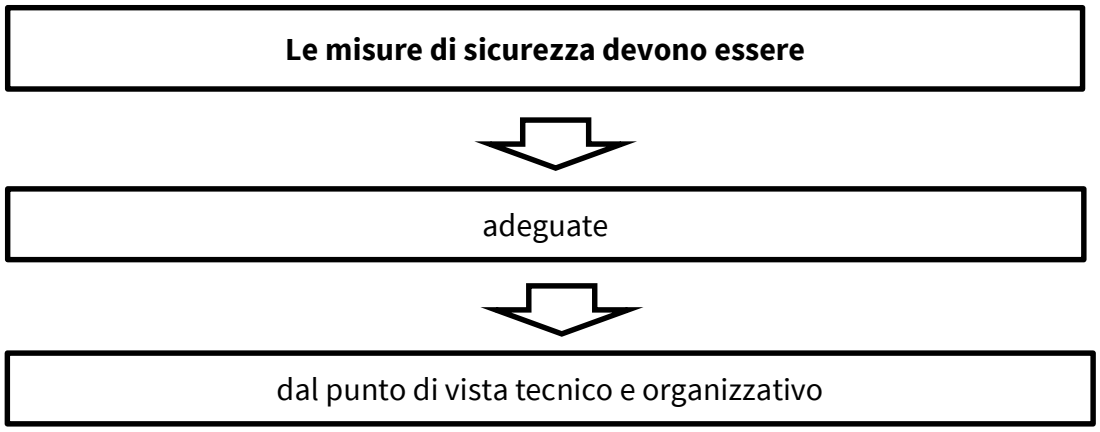
Il sistema impiegato **deve essere programmato in modo da operare, allo scadere del termine previsto, l'integrale cancellazione automatica da ogni supporto delle informazioni**, anche mediante sovra-registrazione, con modalità tali da rendere non riutilizzabili i dati cancellati. Al ricorrere di specifiche esigenze, si può utilizzare il **monitoraggio in tempo reale, che potrebbe presentare dei profili di maggiore rischio rispetto alla memorizzazione e successiva eliminazione automatica del materiale dopo un periodo limitato di tempo.** Per contrastare tale rischio il titolare del trattamento deve conformare l'attività di controllo al principio di minimizzazione.

5.3 LE MISURE DI SICUREZZA

Per quanto riguarda le misure di sicurezza del trattamento, come noto, il GDPR ha eliminato il riferimento alle **misure di sicurezza "minime"**, sostituendolo **con** quello alle **misure tecniche e organizzative adeguate al rischio**, ovvero oggetto di valutazione caso per caso da parte del titolare del trattamento (art. 35, par. 1, del GDPR).

Tra le misure di sicurezza da adottare nel rispetto dei principi di liceità, minimizzazione, esattezza, limitazione della conservazione (art. 5 del GDPR) si riportano:

- previsione di diversi livelli di visibilità delle immagini in base alle differenti competenze dei singoli operatori;
- predisposizione di misure per la cancellazione, anche in forma automatica, delle registrazioni;
- accesso limitato ai soggetti dotati di credenziali di autenticazione abilitanti alla visione delle immagini e, nel caso di interventi di manutenzione, accesso ai dati consentito ai soggetti terzi preposti a tali operazioni solo se ciò si renda indispensabile al fine di effettuare eventuali verifiche tecniche, comunque in presenza di soggetti dotati di credenziali di autenticazione abilitanti;
- applicazione di tecniche crittografiche nel caso in cui le immagini vengano trasmesse su una rete pubblica (internet).



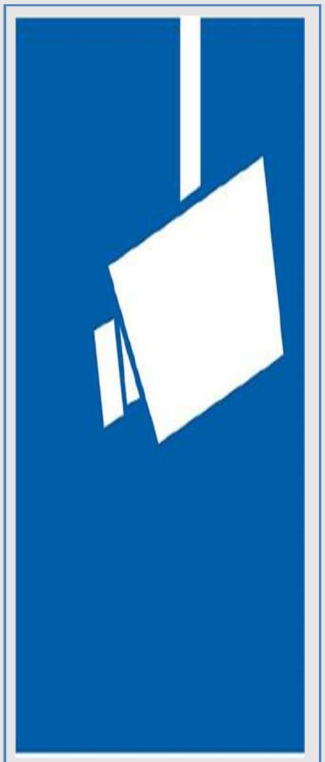
5.4 INFORMATIVA AGLI INTERESSATI

Per garantire un'adeguata informazione agli interessati, in aggiunta all'informativa privacy di cui all'art. 13 del GDPR, è prescritto l'utilizzo di **apposita segnaletica** conforme al modello di informativa "minima", riportante l'indicazione del titolare del trattamento e la finalità perseguita. Tutti i soggetti interessati devono essere consapevoli dell'esistenza e del raggio di azione dell'attività di videosorveglianza nei luoghi monitorati, nel rispetto degli obblighi generali in materia di trasparenza e informazione stabiliti dall'art. 12 del GDPR.

Il Comitato europeo per la protezione dei dati (Ebdp) ha precisato che, alla luce del volume di informazioni che è necessario fornire all'interessato, i titolari del trattamento dei dati possono seguire un approccio a più livelli in cui scelgono di utilizzare una combinazione di metodi per garantire la trasparenza. Per quanto riguarda la videosorveglianza, le informazioni più importanti dovrebbero essere visualizzate sul segnale di avvertimento (primo livello), mentre gli ulteriori dettagli obbligatori possono essere forniti con altri mezzi (secondo livello).

Per il **primo livello di informazione**, nelle linee guida Ebdp 3/2019 viene fornito un esempio di segnaletica che, in combinazione con un'icona grafica, è considerato idoneo a fornire in modo facilmente visibile e intellegibile una panoramica del trattamento previsto come richiesto dall'art. 12, par. 7 del GDPR (vedi figura sotto).

MODELLO SEMPLIFICATO CARTELLO VIDEOSORVEGLIANZA
(EDPB - Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video - adottate il 29 gennaio 2020)



LA REGISTRAZIONE È EFFETTUATA DA .....
CONTATTI DEL RESPONSABILE DELLA PROTEZIONE DEI DATI (se applicabile): ……

LE IMMAGINI SARANNO CONSERVATE PER UN PERIODO DI…

FINALITÀ DELLA VIDEOSORVEGLIANZA
……

L'informativa completa sul trattamento dei dati è disponibile:

- **presso i locali del titolare (reception, casse, ecc.)**
- **sul sito internet (URL)…**
- **altro**

È POSSIBILE ACCEDERE AI PROPRI DATI ED ESERCITARE GLI ALTRI DIRITTI RICONOSCIUTI DALLA LEGGE RIVOLGENDOSI A ……..

Per la tutela degli interessati, **i cartelli segnaletici devono essere sempre collocati prima del raggio d'azione delle telecamere ed essere chiaramente visibili in ogni condizione di illuminazione ambientale**. La segnaletica non deve necessariamente specificare l'esatta ubicazione delle videocamere, ferma restando la chiarezza circa le aree soggette a monitoraggio e il contesto della sorveglianza.

Le linee guida hanno fornito indicazione esemplificativa del contenuto minimo informativo del "primo livello". La segnaletica di avvertimento deve annoverare i dettagli

delle finalità del trattamento, l'identità del responsabile del trattamento e l'esistenza dei diritti dell'interessato, unitamente alle informazioni sui maggiori impatti del trattamento; gli interessi legittimi perseguiti dal responsabile del trattamento (o da una terza parte); i contatti del responsabile della protezione dei dati, meglio noto come "Data Protection Officer".

Le **informazioni del secondo livello** devono essere rese facilmente accessibili all'interessato. Seppure non sia prescritta, a tal fine, una specifica modalità informativa, rendere le informazioni disponibili in modo digitale potrebbe rendere più facile la consultazione da parte degli interessati.

5.5 LE FAQ DEL GARANTE PRIVACY

1) Quali sono le regole da rispettare per installare sistemi di videosorveglianza?
L'installazione di sistemi di rilevazione delle immagini deve avvenire nel rispetto, oltre che della disciplina in materia di protezione dei dati personali, anche delle altre disposizioni dell'ordinamento applicabili: ad esempio, le vigenti norme dell'ordinamento civile e penale in materia di interferenze illecite nella vita privata, o in materia di controllo a distanza dei lavoratori. Va sottolineato, in particolare, che l'attività di videosorveglianza va effettuata nel rispetto del cosiddetto principio di minimizzazione dei dati riguardo alla scelta delle modalità di ripresa e dislocazione e alla gestione delle varie fasi del trattamento. I dati trattati devono comunque essere pertinenti e non eccedenti rispetto alle finalità perseguite. E' bene ricordare inoltre che il Comitato europeo per la protezione dei dati (EDPB) ha adottato le "Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video" allo scopo di fornire indicazioni sull'applicazione del Regolamento in relazione al trattamento di dati personali attraverso dispositivi video, inclusa la videosorveglianza.

2) Occorre avere una autorizzazione da parte del Garante per installare le telecamere?
No. Non è prevista alcuna autorizzazione da parte del Garante per installare tali sistemi. In base al principio di responsabilizzazione (art. 5, par. 2, del Regolamento), spetta al titolare del trattamento (un'azienda, una pubblica amministrazione, un professionista, un condominio…) valutare la liceità e la proporzionalità del trattamento, tenuto conto del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche. Il titolare del trattamento deve, altresì, valutare se sussistano i presupposti per effettuare una valutazione d'impatto sulla protezione dei dati prima di iniziare il trattamento (cfr. FAQ n. 7).

3) Le persone che transitano nelle aree videosorvegliate devono essere informate della presenza delle telecamere?
Sì. Gli interessati devono sempre essere informati (ex art. 13 del Regolamento) che stanno per accedere in una zona videosorvegliata, anche in occasione di eventi e spettacoli pubblici (ad esempio, concerti, manifestazioni sportive) e a prescindere dal fatto che chi tratta i dati sia un soggetto pubblico o un soggetto privato.

4) In che modo si fornisce l'informativa agli interessati?

L'informativa può essere fornita utilizzando un modello semplificato (anche un semplice cartello, come quello realizzato dall'EDPB e disponibile qui), che deve contenere, tra le altre informazioni, le indicazioni sul titolare del trattamento e sulla finalità perseguita. Il modello può essere adattato a varie circostanze (presenza di più telecamere, vastità dell'area oggetto di rilevamento o modalità delle riprese).

L'informativa va collocata prima di entrare nella zona sorvegliata. Non è necessario rivelare la precisa ubicazione della telecamera, purché non vi siano dubbi su quali zone sono soggette a sorveglianza e sia chiarito in modo inequivocabile il contesto della sorveglianza. L'interessato deve poter capire quale zona sia coperta da una telecamera in modo da evitare la sorveglianza o adeguare il proprio comportamento, ove necessario. L'informativa deve rinviare a un testo completo contenente tutti gli elementi di cui all´art. 13 del Regolamento, indicando come e dove trovarlo (ad es. sul sito Internet del titolare del trattamento o affisso in bacheche o locali dello stesso).

5) Quali sono i tempi dell'eventuale conservazione delle immagini registrate?

Le immagini registrate non possono essere conservate più a lungo di quanto necessario per le finalità per le quali sono acquisite (art. 5, paragrafo 1, lett. c) ed e), del Regolamento). In base al principio di responsabilizzazione (art. 5, paragrafo 2, del Regolamento), spetta al titolare del trattamento individuare i tempi di conservazione delle immagini, tenuto conto del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche. Ciò salvo che specifiche norme di legge non prevedano espressamente determinati tempi di conservazione dei dati (si veda, ad esempio, l'art. 6, co. 8, del D.L. 23/02/2009, n. 11, ai sensi del quale, nell'ambito dell'utilizzo da parte dei Comuni di sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico per la tutela della sicurezza urbana, "la conservazione dei dati, delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza è limitata ai sette giorni successivi alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione"). In via generale, gli scopi legittimi della videosorveglianza sono spesso la sicurezza e la protezione del patrimonio. Solitamente è possibile individuare eventuali danni entro uno o due giorni. Tenendo conto dei principi di minimizzazione dei dati e limitazione della conservazione, i dati personali dovrebbero essere – nella maggior parte dei casi (ad esempio se la videosorveglianza serve a rilevare atti vandalici) – cancellati dopo pochi giorni, preferibilmente tramite meccanismi automatici. Quanto più prolungato è il periodo di conservazione previsto (soprattutto se superiore a 72 ore), tanto più argomentata deve essere l'analisi riferita alla legittimità dello scopo e alla necessità della conservazione. Ad esempio, normalmente il titolare di un piccolo esercizio commerciale si accorgerebbe di eventuali atti vandalici il giorno stesso in cui si verificassero. Un periodo di conservazione di 24 ore è quindi sufficiente. La chiusura nei fine settimana o in periodi festivi più lunghi potrebbe tuttavia giustificare un periodo di conservazione più prolungato.

6) È possibile prolungare i tempi di conservazione delle immagini?

In alcuni casi può essere necessario prolungare i tempi di conservazione delle immagini inizialmente fissati dal titolare o previsti dalla legge: ad esempio, nel caso in cui tale prolungamento si renda necessario a dare seguito ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria in relazione ad un'attività investigativa in corso.

7) Quali sistemi di videosorveglianza necessitano di valutazione d'impatto preventiva?

La valutazione d'impatto preventiva è prevista se il trattamento, quando preveda in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per le persone fisiche (artt. 35 e 36 del Regolamento) (per approfondimenti si vedano le "Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679" - WP248rev.01 del 4 ottobre 2017). Può essere il caso, ad esempio, dei sistemi integrati - sia pubblici che privati - che collegano telecamere tra soggetti diversi nonché dei sistemi intelligenti, capaci di analizzare le immagini ed elaborarle, ad esempio al fine di rilevare automaticamente comportamenti o eventi anomali, segnalarli, ed eventualmente registrarli. La valutazione d'impatto sulla protezione dei dati è sempre richiesta, in particolare, in caso di sorveglianza sistematica su larga scala di una zona accessibile al pubblico (art. 35, par. 3, lett. c) del Regolamento) e negli altri casi indicati dal Garante (cfr. "Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679" dell'11 ottobre 2018).

8) Si possono installare telecamere all'interno degli istituti scolastici?

Si rinvia al riguardo alle FAQ sulla scuola disponibili al link https://www.garanteprivacy.it/home/faq/scuola-e-privacy.

9) Il datore di lavoro pubblico o privato può installare un sistema di videosorveglianza nelle sedi di lavoro?

Sì, esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale, nel rispetto delle altre garanzie previste dalla normativa di settore in materia di installazione di impianti audiovisivi e altri strumenti di controllo (art. 4 della l. 300/1970).

6

Altre forme di controllo a distanza

Il capitolo che segue tratta le “altre forme di controllo a distanza” esclusivamente dal punto di vista della normativa sulla privacy.

L’azienda nel caso di installazione di impianti o strumenti di lavoro da cui può derivare anche indirettamente un controllo sulla prestazione dei lavoratori deve sempre verificare, oltre alle regole sulla privacy descritte in questo capitolo, anche che siano rispettati i requisiti/procedure relative all’installazione previsti dalle disposizioni giuslavoristiche indicati nell’articolo 4 della legge 300 del 1970.

In particolare, in caso di utilizzo di impianti o strumenti di lavoro da cui può derivare un controllo a distanza va sempre operata una valutazione giuslavoristica per individuare in quale dei commi 1 e 2 dell’articolo 4 l’azienda si trovi ad operare nel caso concreto, per definire la necessità o meno di ricorrere ad un accordo sindacale o all’autorizzazione dell’ispettorato secondo le previsioni di legge.

6.1 POSTA ELETTRONICA E INTERNET

La posta elettronica e la navigazione sul web rappresentano strumenti di lavoro imprescindibili sui quali il datore di lavoro ha spesso interesse a svolgere attività di controllo a diverso titolo.

La posta elettronica aziendale di tipo nominativo rappresenta il domicilio informatico del dipendente, ovvero uno spazio a sua disposizione in via esclusiva, tanto che la sua invasione costituisce lesione della riservatezza (vedi Corte di Cassazione Sez. Penale, sentenza 31 marzo 2016, n. 13057).

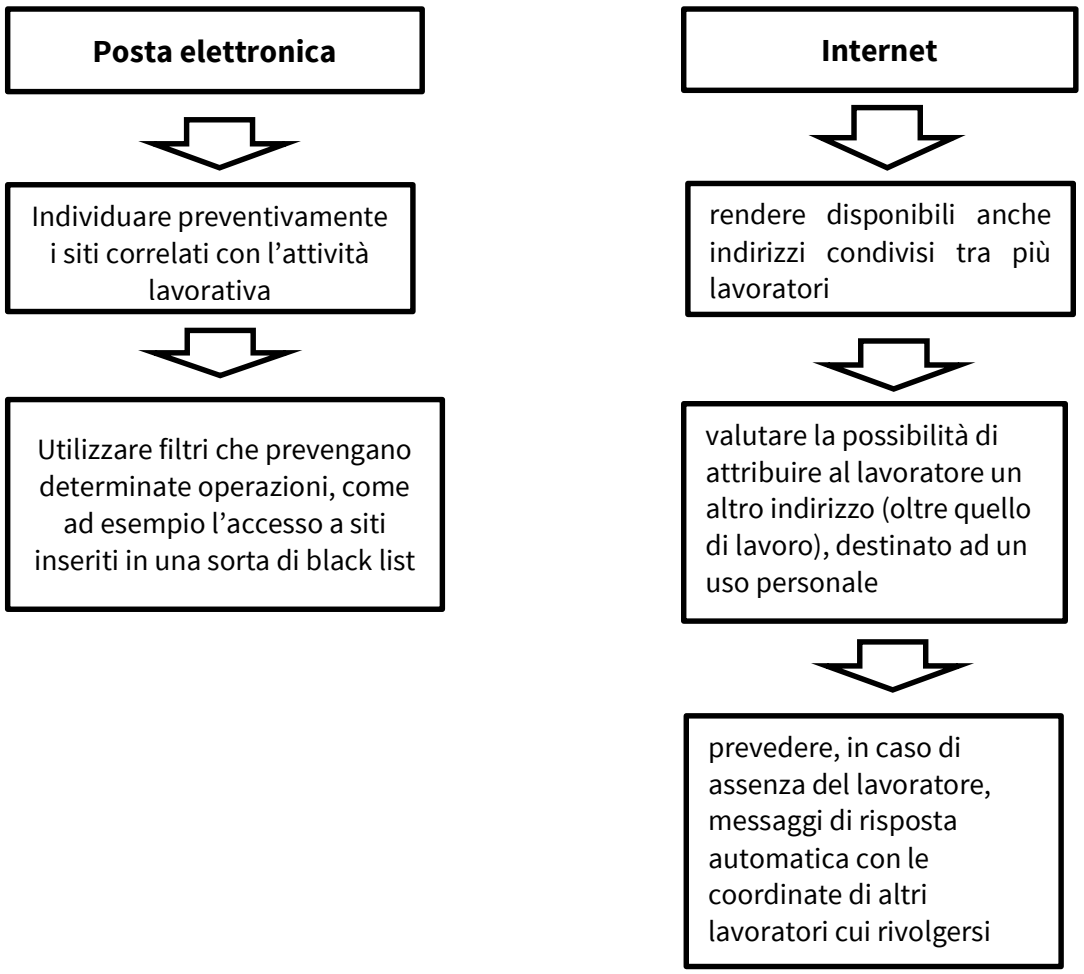
Su entrambi gli strumenti aziendali si applica il generale **divieto di controllo a distanza del lavoratore**, nello specifico divieto di utilizzare software che consentano di ricostruire minuziosamente le attività svolte dal lavoratore. Ad esempio, programmi in grado di leggere e registrare sistematicamente i messaggi di posta elettronica (o dei relativi dati esteriori), al di là di quanto tecnicamente necessario per svolgere il servizio e-mail; software in grado di memorizzare sistematicamente le pagine web visitate dal lavoratore (si vedano "Le Linee Guida del Garante per posta elettronica e internet, deliberazione 13/2007).

Con riferimento ai programmi che consentono **controlli "indiretti"**, questi devono conformarsi ad una **logica di graduazione e**, sulla base dei principi di trasparenza e correttezza del trattamento dei dati, **essere tarati sulla prevenzione di comportamenti non diligenti o contrari alle policy aziendali**.
Il Garante Privacy ha sempre posto l'accento, sia con le linee guida sopracitate che con la sua prassi decisoria, sulla prevenzione piuttosto che sulla repressione, evidenziando come l'adozione di **policy chiare e trasparenti** consenta di trattare correttamente i dati ricavabili dalla posta elettronica e internet in uso al dipendente. In sostanza, il datore di lavoro può scegliere strumenti e modalità che riducano al minimo la capacità intrusiva delle tecnologie nella sfera di riservatezza del lavoratore. Si segnalano a tale scopo:

- l'adozione di policy aziendali volte a disciplinare l'uso della posta elettronica e internet;
- l'individuazione di categorie di siti considerati correlati o meno con la prestazione lavorativa;
- la configurazione di sistemi o l'utilizzo di filtri che prevengano determinate operazioni reputate inconferenti con l'attività lavorativa, quali l'upload o l'accesso a determinati siti (inseriti in una sorta di black list) e/o il download di file o software aventi particolari caratteristiche (dimensionali o di tipologia di dato). Ad esempio, un sistema di black list basato su parole chiave impedirebbe ex ante al lavoratore di accedere ai siti web considerati non correlati con la prestazione lavorativa o illegali;
- uno strumento informatico di prevenzione della perdita dei dati in grado di rilevare un'e-mail in uscita come possibile violazione dei dati (perché trasferisce un database di clienti) e che invii al mittente, prima della trasmissione del messaggio, un avviso che gli permetta di annullare l'invio.

Si evidenziano, inoltre, alcune misure idonee a tutelare la riservatezza del lavoratore:

- rendere disponibili indirizzi di posta elettronica condivisi tra più lavoratori (ad esempio, info@ente.it, ufficiovendite@ente.it, ecc.), eventualmente affiancandoli a quelli individuali (ad esempio, m.rossi@ente.it);
- invio automatico in caso di assenze (ad esempio, per ferie o attività di lavoro fuori sede), di messaggi di risposta contenenti le coordinate di un altro soggetto o altre utili modalità di contatto della struttura, allo scopo di prevenire l'apertura della posta elettronica;
- nei messaggi di posta elettronica, avvertimento ai destinatari nel quale sia dichiarata l'eventuale natura non personale dei messaggi stessi, precisando se le risposte potranno essere conosciute dall'organizzazione di appartenenza del mittente, con espresso rinvio alla policy aziendale;
- la conservazione dei dati relativi agli account aziendali non può svolgersi per tutta la durata del rapporto di lavoro e anche successivamente all'interruzione dello stesso; inoltre, gli account nominativi devono essere disattivati dopo la cessazione del rapporto di lavoro;
- sono vietate tutte quelle attività deputate esclusivamente al controllo a distanza del lavoratore, quali, ad esempio, l'installazione di software in grado di leggere e registrare i caratteri inseriti tramite la tastiera o i movimenti effettuati con il mouse, ovvero l'attivazione di telecamere web e la raccolta di filmati registrati.



6.2 LA GEOLOCALIZZAZIONE

I dispositivi di localizzazione geografica, installati su mezzi o strumenti aziendali o ad uso promiscuo, sono in grado di fornire al datore di lavoro informazioni di tipo statico (la posizione nello spazio) e di tipo dinamico (gli spostamenti nello spazio).

Le informazioni si riferiscono sempre al mezzo (smartphone, tablet, veicolo o altro strumento mobile in dotazione), **ma nel momento in cui rendono identificabile o rintracciabile il lavoratore, anche indirettamente, costituiscono un trattamento dei dati ai sensi della normativa europea**, per cui il datore di lavoro è tenuto ad osservare tutte le prescrizioni generali e specifiche previste dalla legge.

La **base giuridica del trattamento dei dati** connesso all'impiego di dispositivi di geolocalizzazione dei veicoli aziendali è giustificato solo se sussistono le esigenze aziendali qualificate individuate ai sensi dell'art. 4, comma 1, dello Statuto dei Lavoratori, a loro volta rilevanti quale declinazione del **legittimo interesse del titolare del trattamento**. In tal caso l'azienda dovrà anche attuare le procedure previste nell'articolo 4 comma 1.

Ma è possibile che **l'installazione sia prescritta eccezionalmente dalla legge, in questi casi i sistemi di geolocalizzazione sarebbero classificabili alla stregua di strumenti di lavoro** e pertanto, impiegabili liberamente, **senza il rispetto di vincoli procedurali** previsti nell'articolo 4 comma 1 della legge 300 del 1970. Il connesso trattamento dei dati, allo stesso modo, troverebbe legittimazione nell'obbligo legale imposto al datore di lavoro.

In tema di localizzazione dei veicoli è intervenuto il Garante Privacy che ha dato indicazioni su alcune finalità che legittimano il trattamento:

- esigenze di tipo logistico (al fine di impartire tempestive istruzioni al conducente del veicolo);
- elaborazione di rapporti di guida (allo scopo di commisurare il tempo di lavoro del conducente, con la conseguente determinazione della retribuzione dovuta, anche in vista dell'assolvimento degli obblighi legali connessi alla tenuta del libro unico del lavoro);
- calcolo dei costi da imputare alla clientela;
- efficiente gestione e manutenzione del parco veicoli, con effetti vantaggiosi anche sulla sicurezza del lavoro e per la sicurezza della collettività;
- utilizzazione dei dati raccolti in caso di furto del veicolo.

In ossequio al principio di minimizzazione del trattamento e della c.d. "privacy by default", si deve provvedere a configurare il sistema tecnologico in modo che siano trattati, per impostazione predefinita, solo i dati strettamente necessari rispetto alla finalità del trattamento (ad esempio prevedendo la possibilità per il lavoratore di disattivare la localizzazione durante le pause) e non dati ulteriori (quali l'invio di segnali d'allarme in relazione alla velocità del veicolo, o la velocità media del veicolo).

Per quanto attiene i sistemi di localizzazione installati sui veicoli utilizzati per l'esecuzione di prestazioni lavorative, sarà necessario collocare all'interno degli stessi delle **vetrofanie** recanti la dizione di **"veicolo sottoposto a localizzazione"**.

Modello di informativa relativa alla geolocalizzazione del veicolo

Nel caso di dispositivi mobili, il sistema dovrà essere configurato in modo che sia visibile un'icona indicante l'attivazione della funzionalità di localizzazione (vedi anche Provvedimento del Garante Privacy n. 232/2018 *"Verifica preliminare. Trattamento di dati personali mediante un sistema di localizzazione geografica dei dispositivi aziendali"*).

Per quanto riguarda le concrete modalità operative del sistema tecnologico, occorre rispettare il principio di proporzionalità, in riferimento alla periodicità della rilevazione (che non può essere troppo ravvicinata, permettendo la ricostruzione particolareggiata del percorso) e ai tempi di conservazione delle informazioni raccolte (che devono essere proporzionati rispetto agli scopi, anche in considerazione della specifica attività lavorativa svolta, vedi anche Provvedimento del Garante Privacy n. 396/2018 *"Localizzazione di veicoli aziendali*").

È ormai largamente diffuso l'utilizzo di sistemi di localizzazione incorporati in strumenti elettronici portatili, sia aziendali che di proprietà dei lavoratori, adoperati principalmente con finalità di rilevazione delle presenze, anche con funzione combinata di registrazione

delle entrate e delle uscite da lavoro ad inizio e fine turno. La rilevazione delle presenze può costituire, in determinati casi, una finalità legittima della localizzazione, ad esempio nel caso di dipendenti in somministrazione dislocati in varie sedi, attraverso l'utilizzo di un'applicazione *software* installata sui *device* personali dei lavoratori. A tal proposito, il Garante Privacy con il Provvedimento n. 350/2016 - *"Verifica preliminare. Trattamento di dati personali mediante un sistema di localizzazione geografica dei dispositivi aziendali"* - ha stabilito la liceità del trattamento, a condizione che fossero rilevati i soli dati relativi alla sede di lavoro, alla data e all'orario della timbratura virtuale. Non è consentito, invece, il trattamento di dati ultronei quali dati relativi al traffico telefonico, sms, posta elettronica e navigazione web.

La geolocalizzazione

Utilizzo di dispositivi che nel momento in cui rendono identificabile o rintracciabile il lavoratore, anche indirettamente, costituiscono un trattamento dei dati ai sensi della normativa europea

La base giuridica del trattamento dei dati connesso all'impiego di dispositivi di geolocalizzazione dei veicoli aziendali è giustificato legalmente solo in presenza delle esigenze aziendali qualificate ai sensi dell'art. 4, comma 1 (con applicazione delle relative procedure), dello Statuto dei Lavoratori, a loro volta rilevanti quale declinazione del legittimo interesse del titolare del trattamento.

In ossequio al principio di minimizzazione del trattamento e della c.d. "privacy by default", si deve provvedere a configurare il sistema tecnologico in modo che siano trattati, per impostazione predefinita, solo i dati strettamente necessari rispetto alla finalità del trattamento (ad esempio prevedendo la possibilità per il lavoratore di disattivare la localizzazione durante le pause) e non dati ulteriori (quali l'invio di segnali d'allarme in relazione alla velocità del veicolo, o la velocità media del veicolo).

6.3 DISPOSITIVI INDOSSABILI. "RFID (RADIO FREQUENCY IDENTIFICATION)"

Il Garante Privacy si è pronunciato (vedi Provvedimento del 28 febbraio 2019 sul *"Trattamento di dati personali dei dipendenti mediante dispositivi indossabili"*) anche sull'ammissibilità dell'impiego dei dispositivi cc.dd. "RFID (Radio Frequency Identification)", con tecnologia GPS associata ad un braccialetto indossabile dai dipendenti.

Nello specifico, all'esame del Garante è stato sottoposto il caso di un'azienda operante nei servizi di spazzamento su strada che ha implementato un sistema tecnologico in grado di tracciare la collocazione territoriale dei cestini dei rifiuti e, in via indiretta, di identificare i lavoratori addetti al loro svuotamento, attraverso un incrocio tra le informazioni ricavate tramite dispositivo GPS con quelle dei dati dei turni di lavoro. Per la ditta appaltatrice in questione, la localizzazione degli strumenti collegati alla prestazione lavorativa si sarebbe resa necessaria per il rispetto di specifiche obbligazioni contrattuali con l'impresa appaltante, volte a controllare la qualità del servizio erogato. A tal riguardo questi obblighi non influiscono sulla necessità di rispettare, in ogni caso, i principi di liceità, correttezza, trasparenza, finalità, minimizzazione dei dati sanciti dall'art. 5 del GDPR.

Nel Provvedimento, inoltre, si rinvengono alcune indicazioni circa gli accorgimenti da adottare per il trattamento lecito dei dati acquisiti attraverso simili strumenti di localizzazione: in considerazione del rischio di maggiore pervasività di un controllo operato attraverso strumenti tecnologici indossabili; in tal caso la salvaguardia della libertà e dignità del lavoratore richiederà uno standard di protezione maggiormente stringente. Così, il principio di finalità e proporzionalità, richiede l'individuazione dei tempi di conservazione dei dati strettamente necessari rispetto agli scopi perseguiti, nel caso di specie anche avendo riguardo ad eventuali tempistiche relative alle contestazioni di inadempimento, da parte dell'impresa appaltante, di obblighi contrattuali assunti con il conferimento del servizio. Inoltre, dovranno essere indicati preventivamente e tassativamente i casi specifici nei quali si renderà necessario interconnettere le informazioni ottenute per il tramite dei dispositivi di localizzazione con quelli amministrativi (ad esempio registri turni) allo scopo di poter ricostruire fatti oggetto di contestazione.

In sostanza, applicando il principio di minimizzazione dei dati, si consiglia di procedere con opportune modalità che consentano di identificare gli interessati solo in caso di necessità, tenendo presente che l'attività di monitoraggio non può essere continua e la conservazione del dato limitata allo stretto necessario.

Con il Provvedimento in esame, il Garante evidenzia che in tutti i casi in cui vengano installati dispositivi di geolocalizzazione in grado di rendere identificabili i lavoratori, sarà necessario procedere con la **valutazione d'impatto (c.d. "DPIA" ai sensi dell'art. 35 del GDPR)**, ossia un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli.

Le valutazioni d'impatto sulla protezione dei dati sono strumenti importanti per la "responsabilizzazione", in quanto sostengono i titolari del trattamento non soltanto nel rispettare i requisiti del regolamento in generale sulla protezione dei dati, ma anche nel dimostrare che sono state adottate misure appropriate per garantire il rispetto del regolamento.

Dispositivi indossabili "RFID (Radio Frequency Identification)

Principio di minimizzazione dei dati: si consiglia di procedere con opportune modalità che consentano di identificare gli interessati solo in caso di necessità, tenendo presente che l'attività di monitoraggio non può essere continua e la conservazione del dato limitata allo stretto necessario.

6.4 DISPOSITIVI BYOD (BRING YOUR OWN DEVICE)

Nelle aziende tecnologicamente evolute è diffusa la prassi dell'utilizzo di dispositivi portatili personali del lavoratore quali strumenti necessari per l'esecuzione dell'attività lavorativa (telefoni, personal computer, tablet, ecc.).

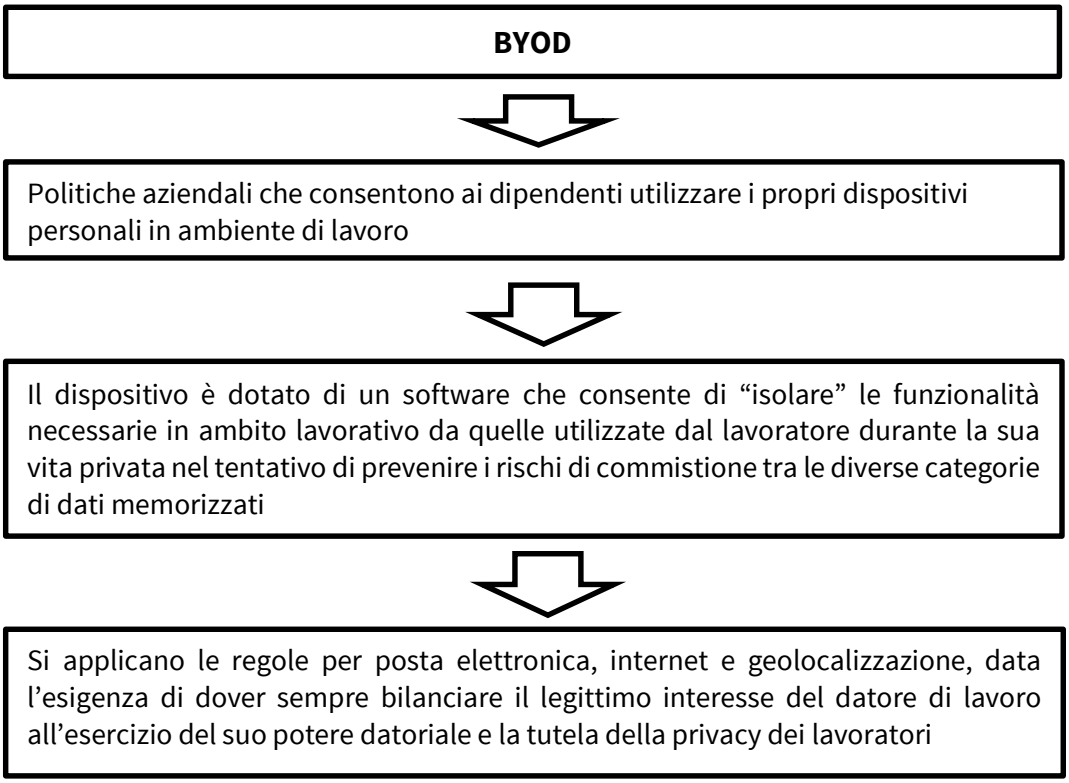
Con l'acronimo **BYOD (Bring Your Own Device)** che in italiano vuol dire **"porta il tuo dispositivo"**, si descrivono tutte quelle politiche aziendali che consentono ai dipendenti di utilizzare i propri dispositivi personali in ambiente di lavoro**. Il dispositivo, in genere, è dotato di un software che consente di "isolare" le funzionalità necessarie in ambito lavorativo da quelle utilizzate dal lavoratore durante la sua vita privata nel tentativo di prevenire i rischi di commistione tra le diverse categorie di dati memorizzati**.

Se con il BYOD il datore di lavoro, da un lato, gode di vantaggi consistenti in termini di abbattimento dei costi per l'acquisto di strumentazione tecnologica e per la realizzazione di attività di formazione e istruzione, dall'altro, la valutazione dell'opportunità della loro adozione è resa alquanto difficile per la necessità di dover implementare adeguati sistemi di sicurezza e protezione dei dati, sia personali che aziendali. Infatti, l'utilizzo "promiscuo" della strumentazione, da un lato, amplifica i rischi di "data breach" (perdita di dati), dall'altro, rende complessa l'attività di controllo del datore di lavoro sui dati e le attività registrate dal dispositivo, in considerazione della quantità di dati sensibili relativi in esso memorizzati e in nessun modo pertinenti all'attività di lavoro.

Tale problematica risulta altresì evidente vista la possibilità offerta dalla normativa vigente di esecuzione della prestazione lavorativa al di fuori del perimetro aziendale. Si pensi al **telelavoro** e al **lavoro agile (smart working)**.
Generalmente, la possibilità di lavorare da remoto implica che il datore di lavoro metta a disposizione tecnologie, quali sistemi cloud o software installati sui dispositivi, che il lavoratore custodisce a casa o in viaggio o comunque in un luogo diverso dalla sede aziendale, al fine di rendere la prestazione lavorativa. È frequente che gli strumenti siano concessi ad uso "promiscuo", anche come benefit individuali, per scopi personali del lavoratore o della sua famiglia, circostanza che ripropone inalterate le considerazioni sui dispositivi BYOD.

A questa forma di esecuzione della prestazione lavorativa si applicano le regole in precedenza illustrate per posta elettronica, internet e geolocalizzazione, data l'esigenza

di dover sempre bilanciare il legittimo interesse del datore di lavoro all'esercizio del suo potere datoriale e la tutela della privacy dei lavoratori.



6.5 DATI BIOMETRICI. LA REGISTRAZIONE DEGLI ACCESSI E DELLE PRESENZE

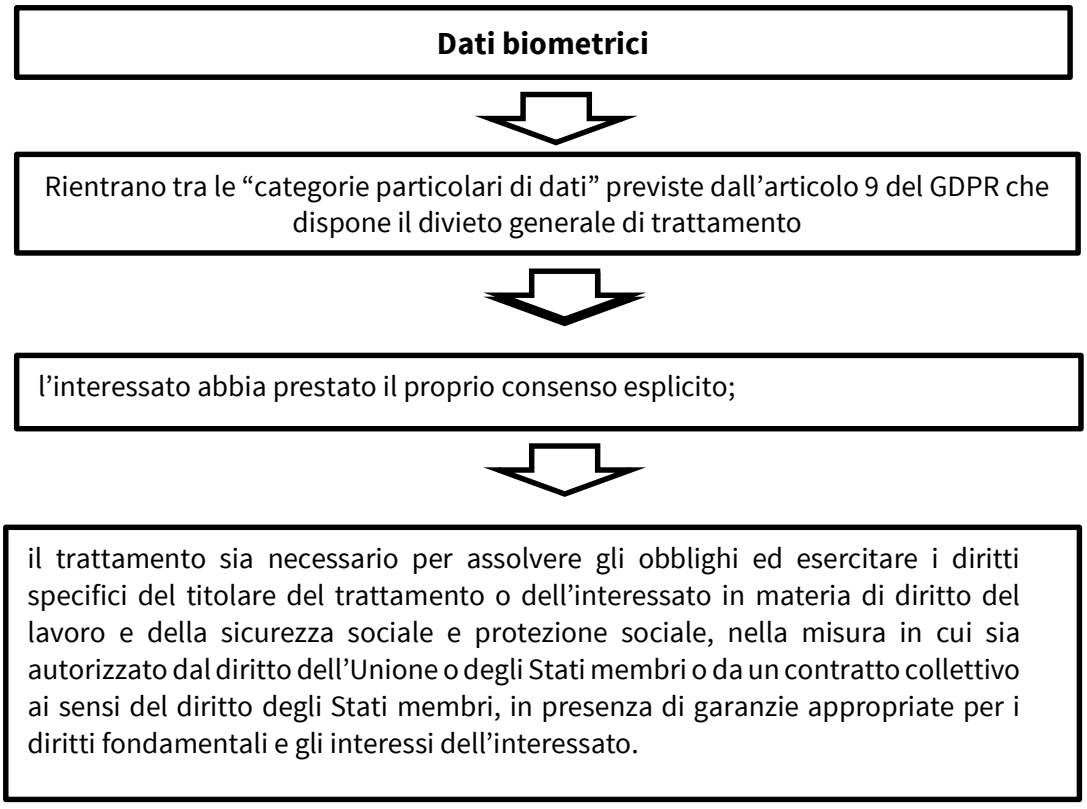
La tecnologia mette a disposizione dei datori di lavoro strumenti sempre più avanzati di controllo degli accessi ad aree aziendali e di registrazione delle presenze dei lavoratori in grado di operare l'identificazione o il riconoscimento degli stessi attraverso dati biometrici come le impronte digitali, la topografia della mano, la fisionomia dei volti, le caratteristiche vocali o dell'iride.

I dati biometrici rientrano tra le "categorie particolari di dati" previste dall'articolo 9 del GDPR che dispone il divieto generale di trattamento, a meno che non si rientri in uno dei casi espressamente previsti dal comma 2 dello stesso articolo 9, ovvero quando:

- l'interessato abbia prestato il proprio consenso esplicito;
- il trattamento sia necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato.

Fatta questa premessa, è sempre necessario che **il datore di lavoro ricerchi mezzi meno invasivi scegliendo, se possibile, un procedimento non biometrico al fine di verificare la presenza del dipendente**, in quanto *"i principi generali di tutela dei dati personali impongono che siano preventivamente considerati altri sistemi, dispositivi e misure di sicurezza fisiche e logistiche che possano assicurare allo stesso modo una puntuale ed attendibile verifica delle presenze e degli ingressi sul luogo di lavoro senza fare ricorso al trattamento dei dati biometrici"* (vedi Provvedimento del Garante Privacy n. 357/2016 "Verifica preliminare. Sistema di lettura di dati biometrici mediante parziale identificazione dell'impronta digitale per la rilevazione della presenza in servizio").

Il Garante Privacy ha ritenuto che il datore di lavoro possa utilizzare la biometria per l'accesso fisico a luoghi ritenuti "sensibili", in cui è necessario assicurare elevati e specifici livelli di sicurezza. Così, ad esempio, un datore di lavoro che installasse tale sistema in una sala server in cui sono conservati, in formato elettronico, dati personali e sensibili dei propri dipendenti, sarebbe perfettamente *compliant* con la normativa che prevede l'obbligo di proteggere tali dati dall'accesso non autorizzato. In tale situazione, in caso di perdita di dati, di anomalie o di accessi non autorizzati, il datore di lavoro potrà legittimamente recuperare le registrazioni conservate allo scopo di individuare i soggetti entrati nell'area riservata. Diversamente, non potrebbe utilizzare la biometria se volesse valutare il rendimento dei dipendenti o monitorarne gli spostamenti all'interno dei locali aziendali.



7

Conclusioni

Il rispetto della privacy riveste una notevole importanza nell'ambito della normativa sul controllo a distanza dell'attività dei dipendenti, come riformulata dal nuovo articolo 4 dello Statuto dei Lavoratori.

Le discipline, da un lato quella giuslavoristica prevista nei commi 1 e 2 e, dall'altro quella privacy richiamata al comma 3 dello stesso articolo, sono tra loro collegate e devono essere sempre entrambe verificate e gestite sui relativi piani dall'azienda.
L'impresa che vuole installare impianti o strumenti di lavoro da cui possa derivare un controllo a distanza ai sensi dell'articolo 4 dovrà quindi verificare sia il rispetto dei requisiti/limiti e procedure imposti dal punto di vista giuslavoristico dai commi 1 e 2, sia controllare il rispetto delle disposizioni in tema di privacy contenute nel comma 3.

La necessità di una gestione parallela dei due diversi piani normativi (giuslavoristico e privacy) è dimostrata dal fatto che accade che ad un controllo a distanza effettuato in ossequio della normativa giuslavoristica non sempre corrisponda un altrettanto rispetto della protezione dei dati personali raccolti (e viceversa), con la conseguenza di non poter utilizzare quest'ultimi per tutti i fini connessi al rapporto di lavoro, ad esempio, perché non è stata resa un'informativa privacy ai dipendenti. Alla stessa conclusione si giunge anche nel caso in cui l'informativa sia stata resa, ma risulti inadeguata o inidonea a rappresentare le finalità e le modalità del trattamento dei dati personali.

In altri termini, dunque, nasce la necessità, per poter utilizzare i dati personali raccolti a tutti i fini connessi al rapporto di lavoro, di attuare un attento e rigoroso rispetto della normativa privacy e, specificatamente, di conformarsi alle finalità e modalità dichiarate, di aggiornare costantemente i processi e la relativa documentazione (in primis l'informativa sul trattamento dei dati personali) in relazione allo sviluppo tecnologico di un dispositivo o a seguito dell'introduzione di un nuovo strumento.

Settore Fisco e Diritto d'Impresa

Il Settore Fisco e Diritto d'Impresa di Assolombarda concorre alla definizione delle posizioni dell'Associazione relativamente alle materie di diritto tributario e legale, fornisce assistenza alle imprese e rappresenta gli interessi imprenditoriali nelle sedi competenti.
Grazie ad un'azione sistematica di informazione consente agli associati di stare al passo con l'evoluzione del quadro normativo, di disporre delle indicazioni necessarie al rispetto degli adempimenti e di compiere scelte gestionali corrette.

Per quanto riguarda **la normativa in materia di protezione dei dati personali**, Assolombarda supporta le imprese nell'applicazione del Regolamento UE n. 679/2016 (GDPR) offrendo loro assistenza con consulenza personalizzata e con informative periodiche in merito all'evoluzione della normativa, alle pronunce del Garante privacy e della Corte di Giustizia dell'UE di maggiore interesse per le imprese.

Organico del Settore

GUIDO MARZORATI
Direttore del Settore
guido.marzorati@assolombarda.it

FRANCESCA AFFINI
francesca.affini@assolombarda.it

MARTA CASTELLI
marta.castelli@assolombarda.it

ALBERTO COLLI
alberto.colli@assolombarda.it

MASSIMO CORTESE
massimo.cortese@assolombarda.it

CARMEN GIUGNO
carmen.giugno@assolombarda.it

MARCO MASSENZ
marco.massenz@assolombarda.it

DOMENICO MISCIOSCIA
domenico.miscioscia@assolombarda.it

PAOLA MONFRINI
paola.monfrini@assolombarda.it

ARMANDO PRIOLO
armando.priolo@assolombarda.it

ELENA TIBERIO
elena.tiberio@assolombarda.it

ANGELO VENTIMIGLIA
angelo.ventimiglia@assolombarda.it

La segreteria
CATERINA DELON – PATRIZIA DAMATO

☎ 02.58370.308 - 02.58370.267
fisc@assolombarda.it

Iscriviti alla newsletter per conoscere le novità normative e interpretative, le scadenze, gli incontri informativi e le notizie pubblicate sul sito. **(Link)**

Elenco Dispense pubblicate

– “Fiscalità delle auto aziendali” N° 01/2021
– “Prescrizione e decadenza nel diritto del lavoro” N° 02/2021
– “Il licenziamento per scarso rendimento” N° 03/2021
– “Le clausole sociali della contrattazione collettiva” N° 04/2021
– “I Comitati Aziendali Europei” N° 05/2021
– “La mobilità internazionale del personale” N° 06/2021
– “Cassa Integrazione Guadagni Straordinaria” N° 07/2021
– “Il premio di risultato” N° 08/2021
– “Dallo smart working nuovi scenari per le sedi aziendali” N° 09/2021
– “I numeri per le risorse umane” N° 10/2021
– “Competitività e Reputazione: quale ruolo gioca la Qualità?” N° 11/2021
– “Il reddito di lavoro dipendente - terza edizione” N° 12/2021
– “Congedi di maternità e paternità Congedi parentali” N° 13/2021
– “IP Lab - Conoscere e valorizzare la proprietà intellettuale in azienda” N° 01/2022
– “L'orario di lavoro” N° 02/2022
– “Cartelle, rateazioni e rottamazione” N° 03/2022

www.assolombarda.it
www.genioeimpresa.it