

La geolocalizzazione del dipendente in smart working: tutela della sicurezza sul lavoro e del patrimonio aziendale o monitoraggio diretto della prestazione lavorativa?

di I. Cartocci – 23 giugno 2025

L'interesse datoriale di controllo sull'attività dei dipendenti al fine di garantire l'esatto e diligente adempimento della prestazione lavorativa (anche tramite l'esercizio del conseguente potere disciplinare) nell'ottica dell'efficientamento produttivo, trova il proprio contraltare nella necessità di tutelare la sfera privata del lavoratore da ogni forma di abusiva interferenza altrui, laddove, ai sensi dell'art. 41 della Costituzione, la libertà d'impresa non può comunque svolgersi in contrasto con l'utilità sociale o in modo da recare danno alla salute, all'ambiente, alla sicurezza, alla libertà, alla dignità umana.

Proprio in ragione dell'esigenza di tutelare il diritto dei lavoratori al rispetto della propria dignità e riservatezza, ove dall'impiego di impianti audiovisivi o di altri strumenti tecnologici per loro natura in grado di invadere agevolmente l'intimità del soggetto controllato derivi la sorveglianza a distanza dei dipendenti, la Legge impone l'osservanza di una serie di limiti e condizioni, in violazione delle quali i dati e le informazioni carpite abusivamente non possono essere utilizzate ai fini dell'applicazione di sanzioni disciplinari.

Ciò in quanto, un incondizionato controllo a distanza, consentirebbe al datore di lavoro di introdursi illecitamente nella vita privata del prestatore di lavoro e accedere ad informazioni confidenziali del tutto estranee allo svolgimento della prestazione lavorativa e ai fini connessi al rapporto di lavoro.

Assumono, dunque, particolare rilevanza i requisiti di liceità della sorveglianza datoriale a distanza sulla prestazione di lavoro dei dipendenti previsti dall'art. 4 dello Statuto dei Lavoratori (così come riformato dall'art. 23 del D. Lgs. 151/2015, c.d. Jobs Act) e dalla competente normativa in materia di privacy (Regolamento UE 2016/679 e D. Lgs. 30 giugno 2003, n. 196, c.d. Codice della Privacy).

Più nel dettaglio, la normativa statutaria prevede che il datore di lavoro possa utilizzare impianti audiovisivi e altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e che tali strumenti possano essere installati solo previo accordo collettivo stipulato con le organizzazioni sindacali o, in mancanza, previa autorizzazione delle articolazioni locali dell'Ispettorato Nazionale del Lavoro territorialmente competente (che non possono mai essere sostituiti dal semplice consenso dei singoli dipendenti, in ragione della natura collettiva del bene giuridico della riservatezza dei lavoratori, oggetto di tutela).

Tutte le informazioni raccolte dal datore di lavoro tramite controllo a distanza, dunque, possono essere utilizzate per tutti i fini connessi al rapporto di lavoro, a condizione che ciò avvenga nel rispetto dei vincoli imposti dalla vigente normativa in materia di privacy e che i prestatori di lavoro ricevano adeguata informazione circa le modalità d'uso degli strumenti ed effettuazione dei controlli.

I suddetti vincoli normativi non si applicano, invece, ai c.d. controlli difensivi posti in essere dal datore di lavoro con lo scopo di accertare specifiche condotte illecite perpetrate da singoli dipendenti anche nel corso della prestazione lavorativa, ove gli accertamenti (anche con strumentazione tecnologica) vengano effettuati *ex post* (ovvero solo dopo che sia maturato un fondato sospetto del comportamento illecito di uno o più lavoratori) e in osservanza dell'obbligo informativo e della normativa in materia di privacy.

Non rientrano, altresì, nel campo di applicazione delle restrizioni di cui all'art. 4 dello Statuto dei Lavoratori i controlli datoriali volti ad ottenere dati e informazioni attinenti all'attività lavorativa dei dipendenti sorvegliati, che vengano effettuati sugli strumenti di lavoro (come, ad esempio, computer, cellulari e tablet) e sui dispositivi di registrazione degli accessi e delle presenze (c.d. lettori badge), purché:

- i lavoratori vengano opportunamente informati sulle modalità d'uso di detti strumenti e sull'esecuzione dei controlli tramite apposito regolamento disciplinare interno;
- non venga violata la normativa competente in materia di privacy;
- gli strumenti consegnati al lavoratore per l'assolvimento delle sue mansioni non vengano modificati (tramite, ad esempio, l'aggiunta di appositi software di localizzazione o filtraggio), volti a verificare la prestazione del lavoratore, divenendo – di fatto – strumenti di controllo a distanza necessitanti la ricorrenza di una delle particolari esigenze aziendali di cui all'art. 4 St. Lav. e dell'accordo sindacale o dell'autorizzazione amministrativa.

In generale, dunque, il datore di lavoro, nell'esercizio del proprio potere di controllo, deve osservare i principi di necessità, correttezza, pertinenza e non eccedenza disposti dalla vigente normativa in tema di privacy.

In particolare, quale titolare del trattamento dei dati personali dei lavoratori, il datore di lavoro deve:

- adempiere opportunamente al proprio onere informativo nei confronti dei dipendenti, con riferimento alle modalità di trattamento dei dati;
- garantire la conservazione dei dati personali al riparo da eventuali trattamenti non autorizzati o illeciti, ovvero dalla perdita, distruzione o danneggiamento accidentale;
- effettuare la preventiva valutazione dei rischi di impatti negativi sulle libertà e i diritti degli interessati derivanti dall'impiego di un determinato sistema di monitoraggio e adottare specifiche misure tecniche e organizzative volte a mitigarli e garantire la trasparenza del trattamento e il rispetto della dignità umana e dei diritti fondamentali dei lavoratori;
- limitare il trattamento dei dati personali alle ipotesi strettamente necessarie alla gestione del rapporto di lavoro e all'adempimento a specifici obblighi o compiti previsti dalla disciplina di settore.

Sulla scia di tali dettami normativi, con il provvedimento n. 135 del 13 marzo 2025 oggetto di esame, si è recentemente espresso il Garante Privacy all'esito di un'approfondita indagine avviata in seguito ad un reclamo presentato da una lavoratrice, condannando una società al pagamento di una sanzione pecuniaria di Euro 50.000,00, per aver posto in essere una serie di controlli a distanza (tramite rilevazione della posizione geografica) nei confronti di 100 dipendenti impegnati nello svolgimento della propria attività lavorativa in modalità agile.

Tale monitoraggio – finalizzato a verificare l'effettiva osservanza del vincolo geografico imposto ai lavoratori con l'accordo individuale di smart working sottoscritto con il datore di lavoro – avveniva mediante un sistema di geolocalizzazione avviato (previo consenso del dipendente), con il quale veniva individuata la posizione del lavoratore controllato “a campione” al momento della doppia timbratura da remoto (in entrata e in uscita) registrata sull'applicazione aziendale ‘Time Relax’ installata sul dispositivo informativo prescelto dal prestatore di lavoro a seguito di accordo sindacale.

In particolare, veniva accertato come, dopo un primo contatto telefonico, nelle fasce orarie di reperibilità, da parte del responsabile dell'unità aziendale preposta a tali controlli, il lavoratore scelto casualmente veniva invitato ad accedere alla suddetta applicazione aziendale ed effettuare la doppia registrazione, nonché a comunicare con successiva e-mail indirizzata allo stesso ufficio di controllo il luogo esatto in cui si trovava al momento delle timbrature.

Eventuali discordanze tra il luogo di lavoro ammesso dal datore di lavoro per lo svolgimento dell'attività da remoto rispetto alla posizione geografica effettivamente risultante dall'applicativo ‘Time Relax’ e/o dichiarata dal lavoratore nell'e-mail sono state, poi, oggetto di specifici procedimenti disciplinari avviati nei confronti dei lavoratori “trasgressori” e conclusisi con l'irrogazione di sanzioni.

L'Ente destinatario del reclamo sosteneva – a propria difesa – il rispetto delle disposizioni statutarie sui controlli a distanza e della normativa vigente in materia di privacy, laddove:

- nel rispetto dell'art. 4 St. Lav., l'accertamento dell'effettivo rispetto del luogo di lavoro prescritto per lo svolgimento dell'attività lavorativa da remoto veniva effettuato esclusivamente in risposta alle esigenze aziendali di garantire la tutela della sicurezza e della salute dei lavoratori esterni ai locali aziendali, nonché di assicurare la riservatezza dei dati e informazioni aziendali rispetto ai maggiori rischi di divulgazione in determinati luoghi accessibili a terzi.
- La procedura di monitoraggio oggetto di reclamo era stata dai lavoratori approvata tramite accordo individuale avente altresì ad oggetto adeguata informativa circa le modalità di effettuazione del controllo a distanza e idoneo consenso informato prestato dai dipendenti al trattamento dei dati anche con riferimento alla geolocalizzazione.
- Per tali ragioni, l'impiego dell'applicazione ‘Time relax’, come una piattaforma di geolocalizzazione esclusivamente ai fini delle operazioni di rilevazione della presenza (timbratura), era stato a monte ratificato a mezzo di accordo con le rappresentanze sindacali, nel pieno rispetto dell'art. 4 della L. 300/1970, unitamente all'approvazione del “Regolamento aziendale del lavoro agile” riportante la predetta funzione di geolocalizzazione.

- Il controllo avveniva – analogamente alla supervisione del personale in presenza – in modo del tutto ipotetico e casuale, mediante avviso telefonico che precedeva la timbratura di verifica e solo nei giorni e nella fascia oraria di contattabilità del dipendente; inoltre, non venivano effettuate ulteriori verifiche durante l’orario di servizio, rilevando l’applicativo la posizione del lavoratore esclusivamente al momento della doppia timbratura e non consentendo la conservazione delle coordinate geografiche; era, poi, richiesto al dipendente il previo consenso alla geolocalizzazione in sede di accesso all’applicazione aziendale (senza il quale non sarebbe possibile la timbratura da remoto nell’ambito del lavoro agile).
- Conformemente a quanto previsto dall’art. 4, comma 3, St. Lav., a tutti i dipendenti interessati era stata data adeguata informazione sulle modalità di esecuzione dei controlli (anche con particolare riferimento alle impostazioni di sicurezza dell’applicazione) e sul trattamento dei dati personali ex art. 13 del Regolamento UE 2016/679 (ivi compresi i soggetti aventi accesso ai dati del lavoro in modalità agile).

Ciò nonostante, il Garante per la protezione dei dati personali – vagliate le argomentazioni adottate dall’Ente – dichiarava illegittimi siffatti controlli a distanza, rilevando come il trattamento dei dati di geolocalizzazione dello smart working per il tramite dell’applicazione ‘Time Relax’, dovessero ritenersi preordinati al perseguimento di finalità non ammesse dalla normativa statutaria, nonché in violazione della normativa privacy di riferimento.

In particolare, il Garante affermava come – indipendentemente dalla presenza di un accordo sindacale (quale condizione necessaria per l’impiego di un determinato sistema da cui derivi il controllo a distanza dei lavoratori e il trattamento dei relativi dati sensibili acquisiti, ma non sufficiente ad assicurare la complessiva liceità del trattamento) – il datore di lavoro, titolare del trattamento, oltre alla normativa di settore applicabile, deve sempre rispettare i principi posti a presidio della riservatezza dei dati personali.

Ciò in quanto, “l’intersezione normativa tra la disciplina in materia di protezione dei dati personali e quella in materia di controlli a distanza dell’attività lavorativa, sebbene risulti idonea ad assicurare una tutela rafforzata del lavoratore, in quanto interessato vulnerabile per effetto dell’asimmetria del rapporto contrattuale con il datore di lavoro, evidenzia la complementarità tra due corpi normativi che restano, tuttavia, tra loro autonomi e distinti”.

A giudizio del Garante, invece, la verifica a distanza dell’osservanza da parte dei lavoratori degli obblighi previsti dall’accordo di smart working con riguardo alla sede dello svolgimento dell’attività lavorativa non è risultata conforme a principi fondamentali del trattamento, ovvero ai principi di “liceità, correttezza e trasparenza”, di “limitazione della finalità”, di “minimizzazione dei dati”, di “protezione dei dati fin dalla progettazione” e di “protezione dei dati per impostazione predefinita”, nonché per mancanza di “idoneo presupposto di liceità”.

Infatti, in ogni caso, l’autorità di controllo – accertato che la lavoratrice reclamante fosse stata invitata ad accedere all’applicazione aziendale per la doppia timbratura anche dopo la sua ammissione, una volta contattata telefonicamente dall’Azienda, “di non trovarsi nel luogo

che aveva originariamente comunicato” – riteneva che tali controlli fossero altresì sprovvisti delle condizioni di garanzia previste dalla legge poiché non avvenuti indirettamente e incidentalmente in occasione del perseguimento di finalità legittime, ma direttamente preordinati alla verifica dell’osservanza da parte del lavoratore degli obblighi discendenti dall’accordo in materia di lavoro in modalità agile con riguardo alla sede dello svolgimento dell’attività lavorativa e utilizzare le informazioni raccolte per fini disciplinari.

A sostegno di ciò, sul punto, ricordava il Garante privacy che *“le diverse esigenze di controllo dell’osservanza dei doveri di diligenza del lavoratore - che pure rientrano nelle prerogative datoriali se perseguite personalmente dal datore di lavoro o attraverso la propria organizzazione gerarchica (articoli n. 2086 e 2104 del codice civile) - non possono invece essere perseguite con strumenti tecnologici a distanza, che, riducendo lo spazio di libertà e dignità della persona in modo meccanico e anelastico, comportano un monitoraggio diretto dell’attività del lavoratore non consentito dall’ordinamento vigente e dal quadro costituzionale.”* [...] *“Ciò comporta che il perseguimento della predetta finalità di controllo diretto non è ammissibile nell’ordinamento neppure in presenza di un eventuale accordo con la rappresentanza sindacale unitaria o con le rappresentanze sindacali aziendali, trattandosi di una finalità che si colloca al di fuori della cornice di garanzia delineata dalle disposizioni di settore e, più radicalmente, dall’assetto costituzionale interno...”*.

Tuttavia – pur ritenendo condivisibile la volontà del Garante privacy di riconoscere preminenza all’interesse di tutela della riservatezza del lavoratore (soprattutto in un contesto lavorativo di maggiore flessibilità spazio-temporale come quello del lavoro in modalità agile, tale da rendere maggiormente labile il confine tra vita privata e professionale) – permangono, a parere di chi scrive, diversi dubbi circa un’interpretazione dell’autorità di controllo talmente stringente da escludere nel caso di specie la sussistenza di un’effettiva esigenza datoriale di tutela della sicurezza dei lavoratori e di protezione dei dati aziendali alla base dei controlli a distanza (resa ancor più pregnante in ambienti di lavoro c.d. “diffusi”).

Diversamente, gli specifici interessi di tutela della sicurezza del lavoratore e del patrimonio aziendale alla base dei suddetti controlli a distanza risultavano perseguiti dall’Ente già in sede di definizione delle condizioni e modalità di svolgimento dell’attività in smart working tramite sottoscrizione di accordo individuale, con il quale – oltre ad assolvere l’onere informativo nei confronti dei lavoratori con riferimento alle modalità di monitoraggio e al trattamento dei dati personali – il datore di lavoro individuava le sedi esterne al contesto aziendale idonee allo svolgimento della prestazione in modalità agile.

E d’altronde, il perseguimento delle suddette legittime esigenze aziendali risulterebbe altresì deducibile dal tenore dei controlli a distanza posti in essere dall’Azienda laddove – come accertato dallo stesso Garante – il dato relativo alla geolocalizzazione del dipendente in smart working (ricavato dal controllo mirato del lavoratore casualmente scelto) veniva trattato esclusivamente all’atto della timbratura da parte del dipendente (in occasione dell’inizio e della fine dell’attività lavorativa) o, comunque, in occasione della fruizione di eventuali permessi di cui il dipendente si avvalsesse nell’ambito della sua fascia di reperibilità.

Ebbene, sul punto, si segnala come l’Ispettorato Nazionale del Lavoro, con nota n. 9728 del 12 novembre 2019, ha ritenuto conforme alla disciplina in tema di controllo a distanza la localizzazione geografica del dipendente tramite applicazione aziendale installata sullo stru-

mento di lavoro, ove il monitoraggio avvenga esclusivamente in un determinato momento (con successiva disattivazione dell'applicativo) e non in modo prolungato, costante, indiscriminato ed invasivo tale da determinare una intollerabile compressione della libertà e dignità dei lavoratori.

Inoltre, la preventiva comunicazione telefonica della violazione dei limiti geografici imposti dall'accordo individuale di smart working da parte della lavoratrice reclamante rispetto alla richiesta mirata di timbratura al fine di accertare l'effettiva discordanza di luoghi segnalata, non rivelerebbe necessariamente – come affermato dal Garante – la precipua finalità disciplinare dell'Ente tramite controllo diretto della prestazione

Difatti, con specifico riferimento al provvedimento disciplinare avviato nei confronti della reclamante, tale monitoraggio postumo, oltre ad essere conforme all'ordine temporale dell'iter ispettivo stabilito dalla prassi aziendale, potrebbe altresì integrare un mirato “controllo difensivo” (che, pur non giustificando un sostanziale annullamento di ogni forma di garanzia della dignità e riservatezza del lavoratore, si situa all'esterno del perimetro applicativo dell'art. 4 St. Lav.), posto in essere in seguito al sorgere di un fondato sospetto della commissione dell'illecito disciplinare da parte della lavoratrice che aveva precedentemente informato l'Azienda al telefono “di non trovarsi nel luogo che aveva originariamente comunicato”.

Ivan Cartocci, avvocato in Milano

Visualizza il documento: [Garante privacy 13 marzo 2025, n. 135](#)