Smart working e privacy: perché l'azienda rischia una multa se usa la geolocalizzazione

di Claudio Garau

Pubblicato il 21 Maggio 2025

Un caso emblematico riporta l'attenzione sul delicato equilibrio tra controllo dei lavoratori e tutela della privacy. Un'azienda è stata sanzionata per aver geolocalizzato i dipendenti in smart working in modo invasivo. Ma oltre alla multa, ciò che conta è il principio affermato sull'equilibrio tra esigenze organizzative e tutela della riservatezza. Un caso emblematico, con risvolti di portata generale: ecco cosa devono sapere imprese e datori per evitare errori costosi e sanzioni anche a cinque cifre.

Smart working e geolocalizzazione: sanzioni per chi viola la privacy dei dipendenti

Aziende e datori di lavoro debbono prestare attenzione non soltanto ai possibili controlli di Ispettorato e Inail, ma anche ai poteri affidati al **Garante Privacy**, una figura che – nel corso del tempo – ha acquisito un rilievo sempre maggiore in riferimento alla protezione della sfera di riservatezza del personale dipendente, intervenendo con sanzioni e ordini correttivi quando le aziende non rispettano la legge vigente. Recentemente un'azienda è stata sanzionata con una multa di 50mila euro, perché colpevole di aver attuato una indiscriminata e pervasiva attività di **geolocalizzazione** dei propri **lavoratori in s***mart working*. Ma, al di là della portata della sanzione in sé, ciò che spicca maggiormente nella vicenda è l'orientamento espresso dall'Authority in materia di protezione dei dati personali. Vediamo allora insieme gli aspetti chiave della vicenda e chiariamo perché la decisione del Garante ha, in verità, una portata generale per una pluralità di casi simili.

La vicenda concreta e le modalità di controllo dei lavoratori da remoto

Nel caso che qui interessa, gli uffici di Piazza Venezia a Roma sono intervenuti a seguito di un reclamo di una dipendente e di una segnalazione da parte dell'Ispettorato della Funzione Pubblica, contro un'azienda regionale che aveva rilevato la **posizione geografica** di circa cento dipendenti durante l'attività lavorativa da remoto. In particolare, il reclamo della donna era scaturito da un **addebito disciplinare** sul presupposto di una:

- asserita inosservanza nei tempi e modalità delle procedure previste dalle regole aziendali, riguardanti lo svolgimento del lavoro in modalità agile;
- rilevata differenza tra il luogo dichiarato nell'accordo individuale di *smart working* e la geolocalizzazione accertata dall'Ufficio Ispettivo nell'espletamento delle verifiche.

Dall'istruttoria è emerso che il datore effettuava un **controllo sistematico e mirato dei lavoratori**, i quali venivano scelti a campione e contattati telefonicamente dall'Ufficio controlli con la richiesta di attivare la geolocalizzazione del pc o dello smartphone, compiendo una timbratura – sia in entrata che in uscita – tramite specifica *app*, e di dichiarare successivamente su mail il luogo in cui - in quel preciso momento - si trovavano fisicamente.

Uso della geolocalizzazione e violazione delle norme vigenti

Come indica l'ordinanza-ingiunzione del 13 marzo scorso, sono varie le violazioni riscontrate dal **Garante** nei confronti di una prassi che, oltre a invadere l'altrui sfera di riservatezza, si caratterizzava anche per la possibilità di procedimenti disciplinari interni, in ipotesi di violazioni delle regole aziendali. Nel provvedimento si indica che l'attività di controllo e il trattamento dei dati personali si sono svolti senza un'opportuna **base giuridica** e di una speciale informativa, ma soprattutto travalicando i limiti normativi posti dal **GDPR** e dal **Codice in materia di protezione dei dati personali** (D.Lgs.196/2003). In particolare, per l'Authority, la geolocalizzazione con *app* smartphone o notebook in uso ai lavoratori da remoto è un trattamento che contrasta con i principi di liceità, correttezza e trasparenza alla base del regolamento UE 2016/679 e del Codice della Privacy (e in particolare i suoi articoli 114 e 115). Ma, a ben vedere, a tutela della riservatezza di chi lavora da remoto c'è anzitutto – e prima ancora - la legge 300/1970, ossia lo Statuto dei lavoratori che – al suo art. 4 – dal titolo *"Impianti audiovisivi e altri strumenti di controllo"* stabilisce che gli **impianti audiovisivi** e gli altri strumenti dai quali derivi anche la **possibilità di controllo a distanza** - anche tramite *app* per cellulare - dell'attività dei lavoratori possono essere installati soltanto con accordo collettivo, e usati esclusivamente per queste finalità:

- esigenze organizzative e produttive;
- sicurezza del lavoro;
- tutela del patrimonio aziendale.

Ebbene, a nulla sono valse le difese dell'azienda regionale. Infatti, secondo il **Garante Privacy** la **geolocalizzazione dei dipendenti** durante il turno di lavoro, per controllare che il luogo di compimento

delle mansioni da remoto coincida effettivamente con una delle sedi previste nell'accordo individuale di *smart working*, non è includibile in una delle ipotesi appena elencate e – conseguentemente - si palesa un **controllo vietato e sanzionabile.** In particolare, l'Authority ha rimarcato che, pur utili alla verifica dell'osservanza degli obblighi di diligenza, gli strumenti tecnologici a distanza..

> *..."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".*

Principi di protezione dei dati personali e rilievo dell'accordo sindacale

Non solo. Anche un anteriore accordo con i sindacati, su questa attività di **controllo per geolocalizzazione,** sarebbe comunque irrilevante, perché manca una delle finalità necessarie per i controlli a distanza di cui all'art. 4 della legge 300/1970. In sostanza il datore di lavoro, che è titolare del trattamento delle informazioni di ogni suo dipendente, deve sempre rispettare tutti i principi di tutela della riservatezza e conseguentemente - si legge nell'ordinanza-ingiunzione - l'eventuale accordo con le rappresentanze sindacali:

> *"in merito all'impiego di un determinato sistema che comporta trattamento di dati personali dei lavoratori costituisce condizione necessaria, ma non sempre sufficiente, per assicurare la complessiva liceità del trattamento e il rispetto dei principi di protezione dei dati personali".*

In particolare, il trattamento dati svolto dall'**azienda regionale** nel caso in oggetto, non è consentito dalle regole generali perché contrasta *"tanto con la disciplina in materia di protezione dei dati personali quanto con quella speciale in materia di lavoro agile"*. Ecco perché il fatto che ci fosse un accordo con le rappresentanze sindacali non ha comunque evitato le conseguenze sanzionatorie per l'azienda. Non solo. Per il **Garante** non può ritenersi rilevante la circostanza invocata dall'azienda, per cui l'app di geolocalizzazione richiedeva il consenso al dipendente per accedere alla posizione. E questo perché, come affermato in molte occasioni dall'Authority (ad es. nel provvedimento 16/2021) il consenso dei dipendenti non rappresenta, in questo contesto:

> *"un valido presupposto di liceità per il trattamento dei dati personali, indipendentemente dalla natura pubblica o privata del datore di lavoro".*

Che cosa cambia

Il Garante Privacy, con il provvedimento n. 135 di poche settimane fa, ha così stabilito che la **geolocalizzazione dei lavoratori in** *smart working* è vietata, in quanto effettuata con strumenti tecnologici a distanza che – di fatto - monitorano invasivamente e condizionano l'attività del lavoratore. In base alle norme interne e europee, ogni azienda - pubblica o privata - non può utilizzare un'applicazione installata sui dispositivi forniti in dotazione, in modo da conoscere la posizione di ogni dipendente da remoto durante l'orario di lavoro. Inoltre, è utile ricordare a tutti i datori che il rispetto della normativa privacy è parte integrante della *compliance* aziendale, proprio come le regole in materia di lavoro e sicurezza. Violare le regole citate significherà esporsi ai possibili accertamenti del Garante Privacy, il quale – tra i suoi poteri – ha anche quello di imporre pesanti sanzioni amministrative pecuniarie e limitazioni o divieti alle attività di trattamento.

NdR: potrebbero interessarti anche... Controlli sui dipendenti: installazione GPS su auto aziendale e limiti Controlli a distanza: quali adempimenti e limiti per le aziende?

Claudio Garau Mercoledì 21 maggio 2025