Il Garante della privacy proibisce alle imprese di geolocalizzare i propri dipendenti durante lo *smart working*

27/05/2025

DIRITTO EUROPEO E DELLA CONCORRENZA, PROTEZIONE DEI DATI E CYBERSECURITY, CONTENZIOSO

Gaspare Roma
Jacopo Piemonte
Adriano Garofalo
Marco Stillo

In data 13 marzo 2025, il Garante per la Protezione dei Dati Personali si è pronunciato[1] sul reclamo con cui una dipendente dell'Azienda regionale per lo sviluppo dell'agricoltura calabrese ("ARSAC") aveva lamentato presunte violazioni in materia di protezione dei dati personali con riferimento allo svolgimento di taluni controlli volti a verificare la compatibilità della posizione geografica dalla quale ella stava svolgendo la propria prestazione lavorativa in *smart working* rispetto a quanto indicato nell'accordo individuale sottoscritto tra la stessa e l'azienda.

Più particolarmente, l'ARSAC aveva adottato un'applicazione denominata "Time Relax" tramite la quale, al momento della timbratura in entrata e in uscita da parte di ciascun dipendente, e previo suo consenso alla geolocalizzazione, acquisiva le coordinate geografiche dello *smartphone* o del pc di quest'ultimo unitamente al suo codice identificativo, alla data e all'ora della timbratura, di modo da verificare che la posizione geografica dalla quale il personale si trovava a lavorare in *smart working* corrispondesse ad una di quelle indicate all'interno di ciascun accordo individuale in materia stipulato con l'azienda. Dopo aver sottoposto la dipendente in questione ad uno specifico controllo, l'ARSAC aveva avviato un procedimento disciplinare nei suoi confronti sulla base di una discordanza tra l'ubicazione dichiarata e la geolocalizzazione accertata

[1] Il provvedimento è disponibile al seguente LINK.

nell'espletamento delle relative verifiche. Il Dipartimento della Funzione Pubblica della Presidenza del Consiglio dei Ministri, pertanto, aveva segnalato al Garante di essere venuto a conoscenza di pratiche che potrebbero risultare in contrasto con la normativa in materia di protezione dei dati personali poste in essere da parte dell'ARSAC.

Il Garante ha preliminarmente rilevato che anche in caso di svolgimento della prestazione lavorativa in *smart working*, l'impiego di strumenti tecnologici da parte del datore di lavoro, dai quali derivi anche la possibilità di controllare a distanza l'attività dei lavoratori, può avvenire esclusivamente per il perseguimento delle tassative finalità previste dallo Statuto dei lavoratori[2]. Per contro, le diverse esigenze di controllo dell'osservanza dei doveri di diligenza del lavoratore, pur rientrando nelle prerogative datoriali se perseguite personalmente dal datore di lavoro o attraverso la propria organizzazione gerarchica, non possono essere realizzate 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. Sul piano della protezione dei dati personali, pertanto, il trattamento in questione risulta sprovvisto di un'idonea base giuridica, ponendosi in contrasto con il principio di liceità, correttezza e trasparenza e con le disposizioni nazionali specifiche di maggior tutela fatte salve dal Regolamento (UE) 2016/679 (*General Data Protection Regulation*, GDPR)[3]. Anche gli stessi trattamenti di dati personali che possono essere lecitamente effettuati dal datore di lavoro[4], tuttavia, non possono assumere carattere massivo e indiscriminato, dovendo al contrario essere effettuati secondo un principio di gradualità e progressività e, dunque, solo previo esperimento di misure meno limitative dei diritti dei lavoratori.

Sebbene, inoltre, la disciplina in materia di protezione dei dati personali e quella in materia di controlli a distanza dell'attività lavorativa si intersechino tra loro, si tratta comunque di due corpi normativi autonomi e distinti. Di conseguenza, oltre alla normativa di settore applicabile, il datore di lavoro, titolare del trattamento, deve sempre rispettare i principi di protezione dei dati personali. L'eventuale presenza di un accordo con le rappresentanze sindacali in merito all'impiego di un determinato sistema che comporta il trattamento di dati personali dei lavoratori, infatti, costituisce condizione necessaria, ma non sempre sufficiente, per assicurare la complessiva liceità del trattamento e il rispetto di tali principi. Né il trattamento in questione può tantomeno ritenersi lecito sul presupposto che la base giuridica sia rappresentata da una delibera dell'ARSAC. Un atto amministrativo

[2] Legge 20 maggio 1970, n. 300, Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale, nei luoghi di lavoro e norme sul collocamento, GU n. 131 del 27.05.1970. L'articolo 4 della Legge, intitolato "Impianti audiovisivi e altri strumenti di controllo", al paragrafo 1 dispone: "*... 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.*
In mancanza di accordo, gli impianti e gli strumenti di cui al primo periodo possono essere installati previa autorizzazione della 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, della sede centrale dell'Ispettorato nazionale del lavoro. I provvedimenti di cui al terzo periodo sono definitivi...".

[3] GUUE L 119 del 04.05.2016.

[4] Ossia quelli a carattere indiretto o preterintenzionale.

generale, infatti, non è in grado di modificare e/o assorbire interamente la disciplina vigente in materia di protezione dei dati personali.

Tutto ciò premesso, pertanto, il trattamento, da parte di ARSAC, dei dati relativi alla posizione geografica del personale che presta la propria attività lavorativa in *smart working* attraverso l'applicazione Time Relax risulta non conforme ai principi di liceità, correttezza e trasparenza nonché di limitazione della finalità. Le caratteristiche dell'applicazione, inoltre, non sono proporzionate rispetto alla finalità perseguita dall'azienda, dando luogo ad una raccolta sistematica di informazioni non necessarie in ragione delle peculiarità dello svolgimento della prestazione in *smart working*. L'esigenza di assicurare che quest'ultima venga effettivamente resa presso le sedi indicate nell'accordo di riferimento, infatti, non può giustificare ogni forma di interferenza nella vita privata dei dipendenti. Di conseguenza, il Garante ha deciso di sanzionare l'ARSAC con un'ammenda pari a 50.000 euro per la

violazione degli articoli 5[5], 6[6], 13[7], 25[8], 35[9] e 88[10] del GDPR nonché dell'articolo 113[11] del Codice della privacy.

In conclusione, il provvedimento in esame richiama l'attenzione dei datori di lavoro sulla necessità di trattare i dati personali dei dipendenti nel pieno

[5] L'articolo 5 GDPR, intitolato "Principi applicabili al trattamento di dati personali", dispone: "*... I dati personali sono:*
a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);
c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);
f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).
Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»)...".
[6] L'articolo 6 GDPR, intitolato "Liceità del trattamento", al paragrafo 1 dispone: "*... Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:*
a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore...".
[7] L'articolo 13 GDPR, intitolato "Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato", ai paragrafi 1-2 dispone: "*... In caso di raccolta presso l'interessato di dati che lo riguardano, il titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:*
a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
b) i dati di contatto del responsabile della protezione dei dati, ove applicabile;
c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
d) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.

In aggiunta alle informazioni di cui al paragrafo 1, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente:
a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
b) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
c) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
d) il diritto di proporre reclamo a un'autorità di controllo;
e) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato...".

[8] L'articolo 25 GDPR, intitolato "Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita", dispone: "*... Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.*
Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.
Un meccanismo di certificazione approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo...".

[9] L'articolo 35 GDPR, intitolato "Valutazione d'impatto sulla protezione dei dati", al paragrafo 1 dispone: "*... Quando un tipo di trattamento, allorché prevede 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 i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi...*".

[10] L'articolo 88, intitolato "Trattamento dei dati nell'ambito dei rapporti di lavoro", dispone: "*... Gli Stati membri possono prevedere, con legge o tramite contratti collettivi, norme più specifiche per assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro, in particolare per finalità di assunzione, esecuzione del contratto di lavoro, compreso l'adempimento degli obblighi stabiliti dalla legge o da contratti collettivi, di gestione, pianificazione e organizzazione del lavoro, parità e diversità sul posto di lavoro, salute e sicurezza sul lavoro, protezione della proprietà del datore di lavoro o del cliente e ai fini dell'esercizio e del godimento, individuale o collettivo, dei diritti e dei vantaggi connessi al lavoro, nonché per finalità di cessazione del rapporto di lavoro.*
Tali norme includono misure appropriate e specifiche a salvaguardia della dignità umana, degli interessi legittimi e dei diritti fondamentali degli interessati, in particolare per quanto riguarda la trasparenza del trattamento, il trasferimento di dati personali nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune e i sistemi di monitoraggio sul posto di lavoro.
Ogni Stato membro notifica alla Commissione le disposizioni di legge adottate ai sensi del paragrafo 1 entro 25 maggio 2018 e comunica senza ritardo ogni successiva modifica...".

[11] L'articolo 113 del Codice, intitolato **"**Raccolta di dati e pertinenza", dispone: "*... Resta fermo quanto disposto dall'articolo 8 della legge 20 maggio 1970, n. 300, nonché dall'articolo 10 del decreto legislativo 10 settembre 2003, n. 276...*".

rispetto dei principi di liceità, correttezza, trasparenza, minimizzazione e proporzionalità, come previsto dal GDPR. Particolare cautela deve essere riservata ai trattamenti automatizzati e all'utilizzo di strumenti tecnologici, come *software* di monitoraggio, *badge* elettronici o sistemi di geolocalizzazione, che possono incidere significativamente sui diritti e le libertà dei lavoratori. È fondamentale, inoltre, che ogni attività di controllo rispetti i limiti posti dallo Statuto dei Lavoratori e sia preceduta da un'adeguata informativa.

Tutto ciò premesso, il provvedimento del Garante dimostra come il raggiungimento di un accordo sindacale non garantisca, di per sé, l'immunità da future contestazioni (come, di fatto, avvenuto nel caso esaminato) e ciò in quanto, come è stato ribadito dal Garante, i due sistemi normativi (protezione dei diritti dei lavoratori e tutela della *privacy*) operano su campi distinti e separati, sebbene interconnessi tra di loro. È pertanto sempre necessario, indipendentemente da eventuali intese sindacali, effettuare un "*double-check*" sugli impatti che la normativa *privacy* potrebbe avere in caso di contenziosi promossi dai dipendenti. In particolare, nei casi di trattamenti ad alto rischio (come la geolocalizzazione di un lavoratore in *smart working*, nel caso di specie), il datore di lavoro è comunque tenuto a effettuare una valutazione d'impatto sulla protezione dei dati[12]. Qualora da tale analisi emerga un'incidenza eccessiva sui diritti fondamentali (e a riguardo, provvedimenti come quello in esame rappresentano un'importante cartina di tornasole), il trattamento non potrà essere attuato. Se si decidesse, comunque, di procedere, la valutazione d'impatto potrà quantomeno dimostrare che la società ha affrontato consapevolmente il problema, assumendosene la piena responsabilità.

In ogni caso, il rispetto della normativa in materia di protezione dei dati personali non solo tutela i diritti dei lavoratori, e bensì costituisce anche un presupposto essenziale per costruire un clima di fiducia e responsabilità all'interno dell'organizzazione. Inoltre, l'avvenuto rispetto delle prescrizioni in materia di trattamento dei dati personali può ben essere anche ripreso e integrato nell'eventuale accordo sindacale ai sensi dell'articolo 4 dello Statuto che, ai fini meramente giuslavoristici, i datori di lavoro sono tenuti a concludere prima di procedere legittimamente con l'attivazione di sistemi di controllo a distanza dell'attività dei lavoratori (quali quelli installati, ad esempio, sugli strumenti informatici di lavoro dei dipendenti in *smart working*).

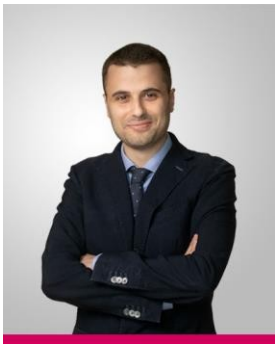
[12] Si veda la nota 9 sopra.

Gaspare Roma
PARTNER

g.roma@dejalex.com
+39 02 72554.1
Via San Paolo 7
20121 - Milano

Jacopo Piemonte
ASSOCIATE

j.piemonte@dejalex.com
+39 02 72554.1
Via San Paolo 7
20121 – Milano
+32 (0)26455670
Chaussée de La Hulpe 187
1170 - Bruxelles



Adriano Garofalo
ASSOCIATE

a.garofalo@dejalex.com
+39 02 72554.1
Via San Paolo 7
20121 - Milano

Marco Stillo
ASSOCIATE

m.stillo@dejalex.com
+39 02 72554.1
Via San Paolo 7
20121 - Milano

MILANO
Via San Paolo, 7 · 20121 Milano, Italia
T. +39 02 72554.1 · F. +39 02 72554.400
milan@dejalex.com

ROMA
Via Vincenzo Bellini, 24 · 00198 Roma, Italia
T. +39 06 809154.1 · F. +39 06 809154.44
rome@dejalex.com

BRUXELLES
Chaussée de La Hulpe 187 · 1170 Bruxelles, Belgique
T. +32 (0)26455670 · F. +32 (0)27420138
brussels@dejalex.com

MOSCOW
Potapovsky Lane, 5, build. 2, 4th floor, office 401/12/9 · 101000, Moscow, Russia
T. +7 495 792 54 92 · F. +7 495 792 54 93
moscow@dejalex.com