COME SI APPLICA IL GDPR AL TRATTAMENTO DATI SUI LUOGHI DI LAVORO?

Il trattamento dati dei dipendenti è uno dei punti più controversi in sede di implementazione degli obblighi "privacy" introdotti dal Reg. UE 2016/679 (GDPR).

Con provvedimento 13 dicembre 2018, il Garante Privacy italiano ha sanzionato una Cooperativa in qualità di datore di lavoro per l'utilizzo di un insolito metodo di valutazione dei dipendenti. Il datore di lavoro ogni settimana affiggeva nella bacheca aziendale un cartello nel quale i volti dei dipendenti erano associati a emoticon che rappresentavano i giudizi, positivi o negativi, espressi dalla cooperativa, nella stessa bacheca erano affisse anche le eventuali contestazioni disciplinari. Il datore di lavoro aveva messo in atto una sorta di "concorso a premi" obbligatorio per i lavoratori, con relativo prelievo mensile dalla busta paga della quota di partecipazione, con pubblicazione nella bacheca aziendale delle valutazioni settimanali, nonché le eventuali contestazioni disciplinari.

Per il Garante tale uso dei dati personali dei lavoratori è illecito in quanto lede la loro dignità, la loro libertà e la loro riservatezza e ne ha quindi vietato l'utilizzo. Nel disporre il divieto il Garante ha ricordato che il datore di lavoro può trattare le informazioni **necessarie e pertinenti** per la gestione del rapporto di lavoro in base a quanto previsto dalle leggi, dai regolamenti, dai contratti collettivi e dal contratto di lavoro individuale. Tra questi non rientrano la sistematica messa a disposizione sulla bacheca aziendale delle valutazioni e dei rilievi disciplinari a tutti i dipendenti e ad eventuali visitatori, tutti soggetti non legittimati a conoscere questo tipo di informazioni, peraltro prima della conclusione del procedimento e in assenza di eventuali repliche degli interessati.

Al di là del caso di specie che sicuramente può considerarsi un interessante esempio "limite" di trattamento dati dei dipendenti, **cosa il datore di lavoro possa o non possa fare ed entro quali limiti, è uno dei punti più controversi in sede di implementazione degli obblighi "privacy" introdotti dal Regolamento UE 2016/679 (GDPR)**.

Le nuove tecnologie, infatti, non solo hanno rivoluzionato il modo di esecuzione delle attività lavorative, ma hanno moltiplicato i trattamenti dati correlati al rapporto di lavoro.

Le comunicazioni dei dipendenti effettuate nei locali aziendali possono rientrare nelle nozioni di "vita privata" e "corrispondenza" ai sensi dell'articolo 8, paragrafo 1, della Convenzione europea dei diritti dell'uomo con l'evidente

inclusione nella lista dei trattamenti dati dei dipendenti operata.

Sul problema il Gruppo di Lavoro Articolo 29 nel Parere 2/2017 " per il corretto trattamento dei dati sul posto di lavoro" ha dato importanti indicazioni sulle best practice da adottare.

Innanzitutto, ai sensi del Regolamento UE 2016/679, i datori di lavoro possono raccogliere dati **soltanto per finalità legittime e il trattamento correlato deve svolgersi in condizioni adeguate** (ad esempio deve essere proporzionato e necessario, attuato a fronte di un interesse effettivo e presente, in maniera lecita, articolata e trasparente) e fondarsi su una base giuridica lecita per il trattamento dei dati personali raccolti o generati tramite comunicazioni elettroniche.

Il fatto che il datore di lavoro sia proprietario delle apparecchiature elettroniche utilizzate non esclude il diritto dei dipendenti alla segretezza delle loro comunicazioni, dei dati relativi all'ubicazione e della corrispondenza.

Per trattare, quindi, correttamente tale dati è importante partire dal **rispetto del principio della trasparenza attraverso una corretta informativa** (art. 13 GDPR) che dovrà riportare anche l'eventuale monitoraggio delle comunicazioni elettroniche, le finalità, le circostanze nelle quali viene svolto, nonché le possibilità dei dipendenti per impedire che i propri dati vengano acquisiti mediante tecnologie di monitoraggio.

È, poi, fondamentale individuare la base giuridica di ciascun trattamento. La maggioranza dei trattamenti dati dei dipendenti dipendono dal **contratto** (es. calcolo delle retribuzioni) o dall'applicazione di una **norma di legge** (es. finalità di calcolo delle imposte e di gestione amministrativa delle retribuzioni, adempimento normativa sulla sicurezza del lavoro). Esistono poi dei trattamenti residuali che possono essere effettuati con il **consenso del dipendente** (es. l'utilizzo dell'immagine per finalità di marketing). Su questi occorre prestare grande attenzione in quanto i dipendenti non sono quasi mai nella posizione di poter concedere, rifiutare o revocare liberamente il consenso al trattamento dei dati, pertanto caso per caso dovrà essere accertata l'effettiva possibilità per il dipendente di rifiutare il trattamento.

In ultimo, ma non meno importante come fondamento giuridico può essere invocato il **legittimo interesse dei datori di lavoro**. In tale base giuridica secondo il Gruppo di lavoro articolo 29 rientrano i trattamenti dati legati al monitoraggio dell'uso degli strumenti aziendali, ma solo se il trattamento è strettamente necessario per conseguire finalità legittime ed è conforme ai principi di proporzionalità e di sussidiarietà. Prima di usare un qualsiasi strumento, quindi, è opportuno effettuare una prova della proporzionalità per valutare se tutti i dati sono necessari, se il trattamento viola i diritti generali alla vita privata di cui godono i dipendenti anche sul posto di lavoro, e le misure da adottare per garantire che le violazioni dei diritti alla vita privata e alla segretezza delle comunicazioni siano limitate al minimo necessario.

Vediamo, quindi i principali esempi pratici di applicazione che il Gruppo di lavoro articolo 29 ha suggerito nel Parere 2/2017.

1. Utilizzo dei dati pubblicati sui social media

Possono aversi due diverse situazioni: il candidato all'assunzione e il dipendente. Vediamole separatamente

Il datore di lavoro potrebbe decidere di acquisire informazioni esaminando i profili social del candidato. Tuttavia, la circostanza che il profilo di una persona sui media sociali è pubblicamente accessibile non ne consente l'automatica utilizzabilità nel processo di selezione. In alcuni casi le informazioni acquisite sui social potrebbe essere utilizzate in quanto ricomprese nel legittimo interesse del titolare, ma sono importanti alcuni accorgimenti. Innanzitutto va distinto il profilo del candidato con finalità professionali da quello strettamente privato, quest'ultime sicuramente di

dubbia ammissibilità. Inoltre, il datore di lavoro dovrà utilizzare i dati personali del candidato solo nella misura siano necessari e pertinenti per l'esecuzione del lavoro per il quale è stata presentata domanda.

Anche l'analisi dei profili del personale assunto non può essere "scontato". Per tutti i profili social vale la considerazione per cui il fatto di essere accessibile pubblicamente non ne autorizza l'immediata utilizzabilità. Sul punto il Gruppo di Lavoro ha dichiarato la propria contrarietà ad uno screening dei profili dei dipendenti sui media sociali avvenire su una base generalizzata.

2. Trattamenti risultanti dal monitoraggio dell'uso delle tecnologie dell'informazione

Tradizionalmente, il monitoraggio delle comunicazioni elettroniche sul posto di lavoro (ad esempio, telefono, navigazione in Internet, posta elettronica, messaggistica istantanea, VOIP, ecc.) è stato considerato la minaccia principale per la vita privata dei dipendenti. È anche possibile che un datore di lavoro implementi una soluzione di monitoraggio "omnicomprensiva", ad esempio un insieme di pacchetti per la sicurezza che gli consentano di monitorare l'utilizzo di tutte le tecnologie dell'informazione e della comunicazione sul posto di lavoro, rispetto al semplice monitoraggio di posta elettronica e/o siti web, come accadeva un tempo.

Partendo dalla oramai generale implementazione di controlli sull'uso degli strumenti informatici, il datore di lavoro dovrebbe preoccuparsi di come questi controlli vengono fatti e di quali dati dei dipendenti interessano, ecco alcuni accorgimenti:

- ove possibile i controlli dovrebbero comunque avvenire in maniera tale da non identificare il dipendente;

- sull'uso di internet il datore di lavoro potrebbe offrire un accesso alternativo non monitorato ai dipendenti, ad esempio offrendo un accesso Wi-Fi gratuito oppure mettendo a disposizione dispositivi o terminali indipendenti (dotati di opportune misure di salvaguardia per garantire la riservatezza delle comunicazioni) tramite i quali i dipendenti possano esercitare il loro legittimo diritto di utilizzare le strutture di lavoro per un determinato uso privato;

- sempre sull'uso di internet il datore di lavoro potrebbe implementare accorgimenti di protezione hardware che prescindano dal controllo dei lavoratori come l'interdizione all'accesso di siti pericolosi per la sicurezza attraverso un firewall o configurare in maniera appropriata l'apparecchio di controllo in modo da non intercettare comunicazioni in circostanze non conformi al criterio di proporzionalità;

- sarà comunque fondamentale la predisposizione di una politica che sia guida sull'uso accettabile e inaccettabile della rete e delle strutture e sulle finalità e modalità di registrazioni sospette.

3. Trattamenti risultanti dal monitoraggio dell'uso delle tecnologie: lavoro a distanza

È diventato sempre più comune per i datori di lavoro offrire ai dipendenti la possibilità di lavorare da remoto, ad esempio, da casa e/o in viaggio. In generale, la possibilità di lavorare da remoto implica che il datore di lavoro rilascia ai dipendenti apparecchiature TIC o software che, una volta installati a casa o sui dispositivi personali, consentono ai dipendenti di avere lo stesso livello di accesso alla rete, ai sistemi e alle risorse del datore di lavoro del quale beneficerebbero se fossero sul posto di lavoro, a seconda del grado di attuazione.

Al fine di attenuare i rischi legati all'assenza delle stesse condizioni di sicurezza tra il lavoro domestico e il lavoro in azienda, i datori di lavoro potrebbero pensare di essere giustificati a utilizzare pacchetti software (sia in modalità locale che nel cloud) in grado, ad esempio, di registrare i tasti premuti e i movimenti compiuti dal mouse,

di acquisire schermate visualizzate (in maniera causale o a intervalli prestabiliti), di registrare le applicazioni utilizzate (e la durata del loro impiego) nonché, su dispositivi compatibili, di attivare telecamere web e raccogliere così filmati registrati.

Tuttavia, **tale trattamento è sproporzionato ed è altamente improbabile che il datore di lavoro disponga di un fondamento giuridico e di un legittimo interesse per registrare, ad esempio, i tasti premuti e i movimenti del mouse compiuti da un dipendente**.

4. Trattamenti risultanti dal monitoraggio dell'uso delle tecnologie dell'informazione: BRING YOUR OWN DEVICE (BYOD)

I datori di lavoro possono trovarsi nella situazione di gestire le richieste di dipendenti che intendono utilizzare i loro dispositivi personali sul posto di lavoro per svolgere i propri compiti: si tratta del "bring your own device" (abbreviato in BYOD), che indica appunto l'utilizzo di propri dispositivi personali.

L'attuazione efficace di questa politica può comportare una serie di vantaggi per i dipendenti, tra cui una maggiore soddisfazione nei confronti del proprio lavoro, un aumento del morale complessivo, una maggiore efficienza sul lavoro e una maggiore flessibilità. Tuttavia, per definizione, il dispositivo del dipendente sarà in parte usato per fini personali, con più probabilità in determinati momenti della giornata (ad esempio la sera e nei fine settimana). Di conseguenza, esiste la possibilità concreta che l'uso di dispositivi propri da parte dei dipendenti comporti un trattamento da parte dei datori di lavoro di informazioni non aziendali relative a tali dipendenti ed eventualmente a qualsiasi loro familiare che utilizzi i dispositivi.

Il monitoraggio dell'ubicazione e del traffico di tali dispositivi può essere – in astratto - considerato rientrare nel legittimo interesse di proteggere i dati personali per i quali il datore di lavoro è responsabile in qualità di titolare del trattamento; tuttavia potrebbe essere illecito quando riguarda un dispositivo personale di un dipendente e permette di acquisire anche dati relativi alla vita privata e familiare del dipendente. Per impedire il monitoraggio delle informazioni private, è necessario che siano attuate misure appropriate per distinguere tra l'uso privato e quello aziendale del dispositivo.

I datori di lavoro dovrebbero altresì attuare sistemi che consentano il trasferimento sicuro, tra il dispositivo del dipendente e la propria rete, dei propri dati presenti sul dispositivo.

In ogni caso, il datore di lavoro deve anche valutare la possibilità di vietare l'uso di dispositivi di lavoro specifici per fini privati qualora non sia possibile impedire il monitoraggio dell'uso privato, ad esempio se il dispositivo in questione consente l'accesso remoto a dati personali per i quali il datore di lavoro è il titolare del trattamento.

5. Trattamenti per la gestione degli orari e presenze

Anche i sistemi che consentono ai datori di lavoro di controllare chi può entrare nei loro locali e/o in determinate aree all'interno degli stessi possono consentire il tracciamento delle attività dei dipendenti. Sebbene tali sistemi esistano da diversi anni, le nuove tecnologie di tracciamento degli orari e delle presenze dei dipendenti sono ora più diffuse, incluse quelle che elaborano dati biometrici e altre quali il tracciamento di dispositivi mobili.

Nonostante tali sistemi possano costituire una componente importante della traccia di controllo di un datore di lavoro, essi presentano anche il rischio di fornire un livello invasivo di conoscenza e controllo in merito alle attività del dipendente sul posto di lavoro.

Dato che è necessario e non viola il diritto alla vita privata dei dipendenti, il trattamento può essere svolto in virtù di un legittimo interesse a norma dell'articolo 7, lettera f), purché i dipendenti ne siano adeguatamente informati. Tuttavia, il

monitoraggio continuo della frequenza e degli orari precisi di entrata e uscita dei dipendenti non può essere giustificato se tali dati vengono utilizzati anche per altre finalità, quali ad esempio la valutazione del rendimento dei dipendenti.

6. Trattamenti dati nell'uso dei veicoli utilizzati dai dipendenti

Le tecnologie che consentono ai datori di lavoro di monitorare i propri veicoli sono attualmente ampiamente adottate in particolare nel contesto di organizzazioni che svolgono attività di trasporto o che dispongono di flotte notevoli di veicoli.

Qualsiasi datore di lavoro che utilizzi dispositivi telematici a bordo di veicoli raccoglierà dati in merito al veicolo e al singolo dipendente che utilizza tale veicolo. Tali dati possono includere non solo la posizione del veicolo (e quindi del dipendente) raccolta dai sistemi di tracciamento di base GPS, ma anche molte altre informazioni, a seconda della tecnologia, compreso il comportamento di guida. Talune tecnologie possono altresì consentire un monitoraggio continuo tanto del veicolo quanto del conducente (si pensi ad esempio ai registratori di dati relativi ad eventi).

Un datore di lavoro potrebbe essere tenuto a installare tale tecnologia di monitoraggio a bordo dei veicoli per dimostrare la conformità ad altri obblighi legali, ad esempio per garantire la sicurezza dei dipendenti che guidano tali veicoli. Il datore di lavoro può anche avere un legittimo interesse a poter individuare i veicoli in qualsiasi momento.

Nonostante il legittimo interesse è necessario valutare se il trattamento per dette finalità sia necessario e se l'effettiva attuazione sia conforme ai principi di proporzionalità e sussidiarietà. Qualora sia consentito l'uso privato di un veicolo professionale, la misura più importante che un datore di lavoro può adottare per garantire il rispetto di tali principi consiste nell'offrire un'opzione di disattivare il dispositivo quando utilizza l'auto per motivi personali.

Resta, invece l'obbligo del datore di lavoro di informare con chiarezza i dipendenti che a bordo del veicolo aziendale è stato installato un dispositivo di tracciamento e che i loro movimenti vengono registrati durante l'uso del veicolo.

È anche importante ricordare quanto indicato nel parere 13/2011 del Gruppo di lavoro articolo 29 sui servizi di geolocalizzazione su dispositivi mobili intelligenti:

"*I dispositivi di tracciamento dei veicoli non sono dispositivi di tracciamento del personale, bensì la loro funzione consiste nel rintracciare o monitorare l'ubicazione dei veicoli sui quali sono installati. I datori di lavoro non dovrebbero considerarli come strumenti per seguire o monitorare il comportamento o gli spostamenti di autisti o di altro personale, ad esempio inviando segnali d'allarme in relazione alla velocità del veicolo*".

Nel trattamento dati in ambito lavorativo sono due le fonti normative e gli obblighi da tenere in considerazione. Il primo è quanto previsto dal provvedimento del Garante "Prescrizioni relative al trattamento di categorie particolari di dati nei rapporti di lavoro (aut. gen. n. 1/2016)". Tale provvedimento, tuttavia, emesso con la normativa previgente è in fase di revisione a seguito dell'entrata in vigore del Regolamento 2016/679.

Il secondo sono gli aspetti relativi al "controllo dei lavoratori" del Job Act.

L'articolo 88 del Regolamento UE 2016/679 stabilisce che gli Stati possono emanare regole particolari atte a garantire la protezione dei diritti e delle libertà dei dipendenti durante i trattamenti dei dati nel contesto del rapporto di lavoro. Questo può avvenire tramite accordi collettivi o disposizioni legislative. Il GDPR prevede, quindi, che le attività di controllo del lavoratore siano svolte in un contesto di trasparenza e di adeguata protezione dei dati personali.

In Italia la regolamentazione in materia è dettata dal D. Lgs n. 151 del 14 settembre del 2015 (Jobs Act) che ha riscritto l'art. 4 dello Statuto dei Lavoratori. Il Jobs Act ha stabilito un regime diverso a seconda del tipo di strumento:

- strumenti che consentono il controllo del lavoratore (es. videosorveglianza);

- strumenti di lavoro (personal computer, smartphone).

Senza entrare nel merito delle singole disposizioni che esulano dalla presente trattazione, si consiglia di verificare sempre la legittimità dell'installazione di uno strumento che consente anche il controllo del dipendente sia sotto il profilo del trattamento dei dati, con gli accorgimenti e le specifiche riportate in questo approfondimento, sia sotto il profilo della compatibilità con quanto previsto dallo Statuto dei lavoratori.

Fonti principali

Pubblicazione in bacheca di dati relativi a contestazioni disciplinari e valutazioni dei soci lavoratori - 13 dicembre 2018 [9068983]

Parere 2/2017 sul trattamento dei dati sul posto di lavoro adottato l'8 giugno 2017

Provvedimento che individua le prescrizioni contenute nelle Autorizzazioni generali nn. 1/2016, 3/2016, 6/2016, 8/2016 e 9/2016 che risultano compatibili con il Regolamento e con il d.lgs. n. 101/2018 di adeguamento del Codice - 13 dicembre 2018 [9068972]