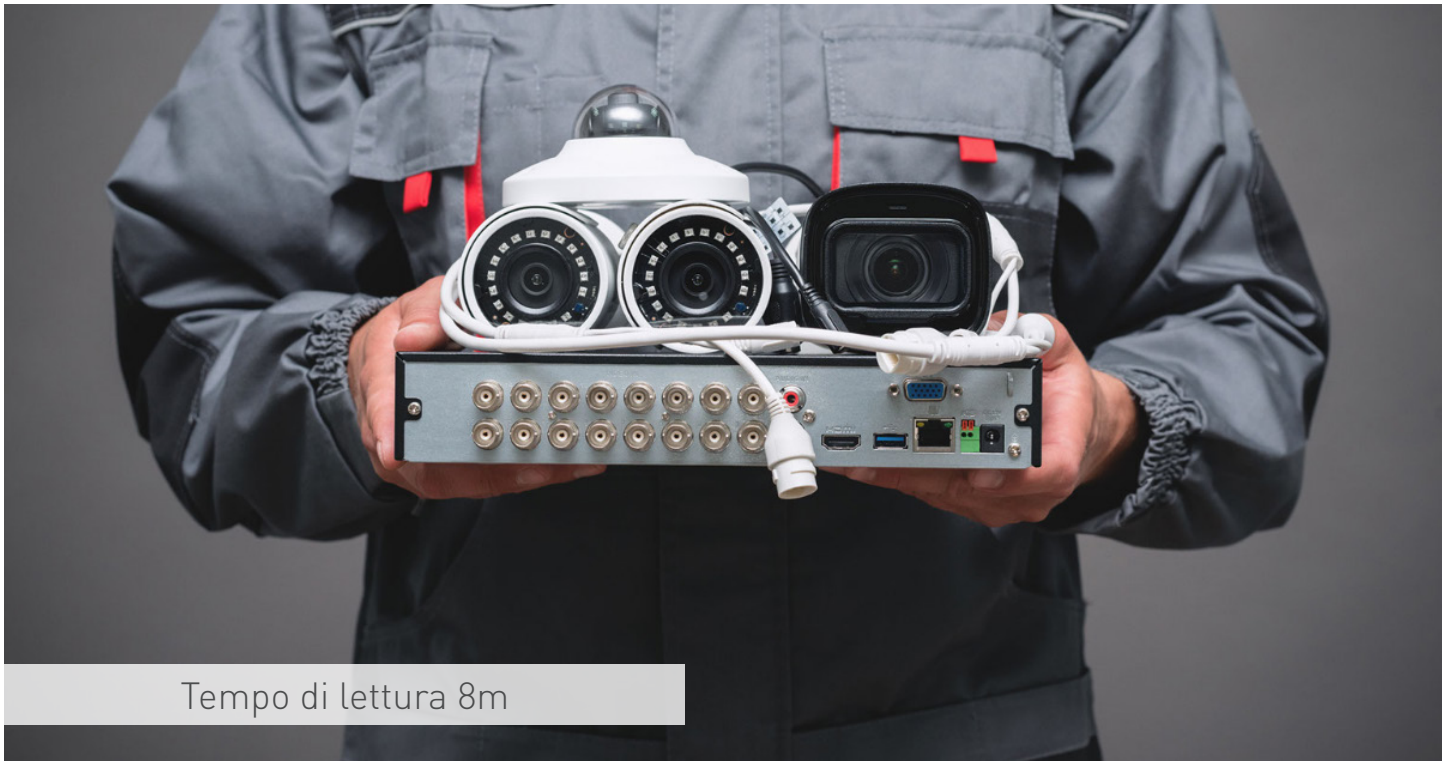
[E03.2022]

PRIVACY E CONTROLLI SULL'ATTIVITÀ LAVORATIVA DEI DIPENDENTI

L'EDITORIALE

08
02
22

CTP
CECCATO
TORMEN
& PARTNERS
CONSULENTI DEL LAVORO



Tempo di lettura 8m

PRIVACY E CONTROLLI SULL'ATTIVITÀ LAVORATIVA DEI DIPENDENTI: L'ART. 4 ST. LAV. NON BASTA QUALE BASE DI LEGITTIMITÀ

È noto che l'art. 4 St. lav. subordina la possibilità di controllo dei lavoratori ad un apposito accordo sindacale o autorizzazione dell'ITL, atti non necessari ove il monitoraggio avvenga sugli strumenti utilizzati dal lavoratore per svolgere la propria prestazione.

La norma, tuttavia, richiede che qualsiasi attività di controllo rispetti le disposizioni del Codice privacy.

Che cosa significa? Come conciliare esigenze di controllo e privacy dei dipendenti? Cosa deve fare il datore di lavoro per non incorrere in alcuna violazione?

Utili indicazioni al riguardo ci vengono fornite dall'Ordinanza-ingiunzione resa dal Garante privacy nei confronti del Comune di Bolzano il 13 maggio 2021. Vediamola insieme.

IL CASO

Un dipendente del Comune di Bolzano aveva adito il Garante privacy lamentando un illecito trattamento dei dati personali posto in essere dal Comune nel monitorare la navigazione Internet. Il lavoratore, in particolare, era stato sanzionato disciplinarmente poiché, dai controlli effettuati, era emersa il suo accesso, per ore, ai social network.

Il Comune si difendeva adducendo di aver stipulato, in proposito, un accordo sindacale inerente al monitoraggio del

traffico di rete per esigenze di sicurezza della propria rete IT, il quale prevedeva altresì che i dirigenti potessero chiedere all'amministratore di rete controlli mirati degli accessi ad internet da parte di personale del rispettivo ufficio.

L'Amministrazione inoltre affermava di aver informato i dipendenti riguardo al monitoraggio del traffico ed alle sue modalità attraverso la pubblicazione di vari documenti, disponibili ai lavoratori: un'informativa generale per i lavoratori sul trattamento dei dati personali; l'accordo sindacale citato, il modulo che ogni dipendente doveva firmare quando faceva richiesta di accedere ad Internet; il codice di comportamento e le circolari interne dell'Ufficio del personale.

LA POSIZIONE DEL GARANTE

Dagli accertamenti del Garante emergeva che il Comune aveva impiegato un sistema di controllo e filtraggio della navigazione internet dei dipendenti, con la conservazione dei dati per un mese e la creazione di apposita reportistica, per finalità di sicurezza della rete.

Il Garante rilevava l'illiceità del trattamento alla luce del Reg. 679/2016/UE, sulla base di alcune considerazioni.

In primo luogo, il titolare del trattamento deve adottare misure appropriate per fornire all'interessato tutte le informazioni di cui agli artt. 13 e 14 del Regolamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro. Nel corso delle verifiche era emerso che, sul sito web dell'Ente, non era presente alcuna specifica informativa relativa ai trattamenti dei dati personali dei dipendenti né, in quelle rese disponibili, vi era alcun riferimento al trattamento dei dati personali relativi alla navigazione in Internet da parte degli stessi. Gli altri atti a disposizione dei dipendenti, in cui veniva menzionato il controllo sulla navigazione Internet, non erano idonei a rivestire valore di informativa ai sensi dell'art. 13 del Regolamento, poiché non contenevano gli elementi essenziali previsti dal GDPR ed erano stati redatti per assolvere ad obblighi diversi rispetto a quelli derivanti dalla disciplina in materia di protezione dei dati. Invece, prima del trattamento il titolare deve rendere agli interessati apposita informativa in merito alle caratteristiche essenziali dello stesso; ciò allo scopo di consentire all'interessato di esser pienamente consapevole della tipologia di operazioni di trattamento che potranno essere svolte anche attingendo, in un quadro di liceità, ai dati raccolti nel corso dell'attività lavorativa.

Inoltre, il titolare del trattamento deve sempre rispettare i principi di protezione dei dati previsti dall'art. 5 del Regolamento, per cui i controlli e i trattamenti di dati personali devono essere comunque non massivi, graduali e ammissibili solo previo esperimento di misure meno limitative dei diritti lavoratori. Dall'istruttoria, era invece emerso che le caratteristiche originarie del sistema e le conseguenti operazioni di trattamento (raccolta preventiva e generalizzata di dati relativi alle connessioni ai siti web dei singoli dipendenti, memorizzazione per trenta giorni e possibilità di estrazione di reportistica relativa alla navigazione di singoli dipendenti) non fossero necessarie e proporzionate rispetto alla finalità di protezione e sicurezza della rete interna invocata dall'Ente.

Inoltre, in linea più generale, il sistema utilizzato dal Comune comportava inevitabilmente il trattamento di informazioni anche estranee all'attività professionale, desumibili dagli URL visitati, e risultava pertanto in contrasto con il divieto per il datore di lavoro di trattare dati "non attinenti alla valutazione dell'attitudine professionale del lavoratore", secondo quanto stabilito dall'art. 113 del Codice, dall'art. 8 della l. 20 maggio 1970, n. 300 e all'art. 10 del d.lgs. 10 settembre 2003, n. 276.

Peraltro, l'art. 4, commi 1 e 2, della l. n. 300/1970 prevede che i dati raccolti attraverso gli strumenti di controllo e quelli di lavoro possano essere utilizzati dal datore di lavoro "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". Quindi, le successive ed eventuali operazioni di trattamento presuppongono la necessità di fornire agli interessati un'adeguata informativa sui trattamenti che il datore di lavoro si riserva di effettuare e l'opportuna configurazione dei sistemi in modo che siano poste in essere le sole operazioni necessarie e raccolti i soli dati pertinenti in relazione alla finalità principale per la quale i dati sono originariamente trattati.

L'art. 88 del GDPR, in aggiunta, consente al datore di lavoro di utilizzare i dati personali dei lavoratori per ulteriori finalità riconducibili all'ambito della gestione del rapporto, ma nei limiti in cui l'originaria raccolta sia stata lecitamente effettuata, avuto riguardo alla finalità principale e nel rispetto dei principi generali della protezione dei dati.

Pertanto, in attuazione del principio di responsabilizzazione, spetta al titolare valutare se i trattamenti che si intendono realizzare possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, che renda necessaria una preventiva valutazione di impatto sulla protezione dei dati personali. Secondo il Garante, un trattamento consistente nella raccolta preventiva e generalizzata di dati relativi alle connessioni ai siti web dei singoli dipendenti, nella memorizzazione per trenta giorni e nella possibilità di estrarre una reportistica relativa alla navigazione di singoli dipendenti, comporta rischi specifici per i diritti e le libertà degli interessati nel contesto lavorativo.

Alla luce dei principi enunciati, la decisione del Garante deve essere tenuta ben presente nell'effettuare operazioni di controllo sull'attività resa dai lavoratori, dato che l'art. 4 St. lav., per se stesso, non vale a legittimarla.

Di conseguenza, sarà necessario:

a. Rendere ai dipendenti apposita informativa, ai sensi dell'art. 13 GDPR, che riguardi specificamente tutti i possibili trattamenti svolti. Non basta, al riguardo, un documento generico;

b. Effettuare la valutazione d'impatto sui trattamenti posti in essere.

CTP

CECCATO TORMEN & PARTNERS CONSULENTI DEL LAVORO

ceccatotormen.com

/ceccatotormen

info@ceccatotormen.com

ceccatotormen@pec.it

Abano Terme PD - Treviso TV

+39 049 7968508