PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 25 - numero 5501 di Venerdì 10 novembre 2023

Protezione dei dati e monitoraggio dei lavoratori

Un documento prezioso per tutti i datori di lavoro, che sono anche titolari del trattamento di dati personali: le linee guida "Data protection and monitoring workers".

L'information Commissioner Office del Regno Unito, vale a dire l'autorità garante per la protezione dati personali, ha pubblicato all'inizio di ottobre una preziosa linea guida, indirizzata a tutti i datori di lavoro, che sono anche titolari del trattamento di dati personali dei dipendenti e collaboratori. Questa linea guida offre puntuali indicazioni sulle attività di monitoraggio, che sono compatibili con la vigente regolamentazione in materia di dati personali.

Questa linea guida, pubblicata il 3 ottobre 2003, è indirizzata ai datori di lavoro, sia pubblici sia privati, e offre una serie di preziose indicazioni su come sia possibile monitorare le attività dei dipendenti, soprattutto in questo periodo, in cui la prestazione lavorativa a distanza diventa sempre più frequente e nuove tecnologie sono disponibili per il controllo dei dipendenti.

La guida mette subito in evidenza che, perché un monitoraggio possa essere legittimo e corretto, deve tenere conto delle attese dei dipendenti, non deve essere eccessivo e deve essere effettuato in modo trasparente, ogniqualvolta possibile.

Ad esempio, quando si consente al dipendente di svolgere la propria attività a distanza, dal proprio domicilio, è del tutto logico che il dipendente ritenga di poter esigere un ben maggiore livello di protezione dei suoi dati, rispetto all'attività svolta in ufficio.

Ovviamente il livello di monitoraggio dipende dall'attività svolta. Ad esempio, dagli operatori che lavorino in una miniera ci si aspetta che indossino dei dispositivi di tracking, per mettere sotto controllo i rischi di incidenti, mentre un tale dispositivo per un dipendente che lavori a domicilio non avrebbe senso.

La linea guida raccomanda inoltre ai titolari del trattamento di prestare molta attenzione all'utilizzo di applicativi decisionali automatici; ad esempio, il fatto che lo stipendio sia collegato alla produttività, monitorata da applicativi automatici, rappresenta una chiara violazione del regolamento generale in materia di protezione dei dati personali.

È per contro consentito l'utilizzo di sistemi automatizzati di supporto alle decisioni, a condizione che la decisione finale venga assunta dal dipendente e non dall'applicativo.

Ad esempio, nulla impedisce che vengano utilizzati degli applicativi che mettono in evidenza l'assenza di dati o la presenza di dati non corretti, nel corso di attività di introduzione dati svolta dai dipendenti, sia a domicilio, sia sul posto di lavoro.

La linea guida presta particolare attenzione anche l'utilizzo di dati biometrici, allineandosi con l'indicazione più volte date anche dalla nostra autorità garante. L'utilizzo di dati biometrici è consentito, ma solo dopo aver effettuato un'accurata analisi dei rischi e verificata la possibilità di utilizzare soluzioni diverse, per raggiungere lo stesso obiettivo

Inoltre, occorre ricordare che, ogniqualvolta si utilizza un applicativo a base biometrica, occorre sviluppare un documento che effettui una valutazione di impatto, in conformità all'articolo 25 del regolamento europeo.

Un capitolo particolarmente interessante è dedicato al controllo della posta elettronica dei dipendenti.

Un esempio illuminante è il seguente:

-nulla impedisce ad un istituto finanziario di controllare tutti i messaggi di posta elettronica, movimentati da un dipendente, quando tali messaggi fanno riferimento a transazioni finanziarie. Il controllo di queste transazioni è indispensabile per mettere in evidenza possibili frodi o situazioni anomale.

Completamente diversa è la situazione, nella quale invece l'applicativo tiene sotto controllo qualunque tipo di messaggio elettronico scambiato dal dipendente, perché in questo caso è evidente che si può entrare in una fase troppo invasiva e non compatibile con gli attuali regolamenti.

Per quanto riguarda gli aspetti di trasparenza e fiducia reciproca, il datore di lavoro viene incoraggiato a prendere nota delle osservazioni, che possono essere fatte dalle rappresentanze sindacali, per garantire una migliore è più corretta comprensione delle attività di monitoraggio in corso.

Occorre inoltre attivare un rapido ed efficiente sistema di risposta a possibili richieste di accesso ai dati, che possano essere avanzate dal dipendente.

Estrema attenzione va posta poi all'attivazione di sistemi di registrazione audio e video, per i gravi rischi connessi alla invasività di queste attività. Ovviamente questi rischi sono accettabili, quando la finalità della registrazione audio e video è quella di tutelare il dipendente, che potrebbe operare in condizioni specifiche di rischio.

Data protection and monitoring workers (pdf)

Adalberto Biasiotti

---

www.puntosicuro.it