Come avviene il controllo degli accessi a lavoro?

written by Redazione | 29/03/2022

Il Garante della privacy ha fornito importanti chiarimenti in merito ai nuovi sistemi di utilizzo dei dati biometrici dei dipendenti sul riconoscimento facciale.

Come avviene il controllo degli accessi a lavoro? Il datore di lavoro può predisporre degli strumenti di controllo delle presenze dei dipendenti tramite registrazione degli accessi e delle uscite, senza bisogno del previo accordo coi sindacati a patto che:

- sia stata data al lavoratore adeguata informazione circa le modalità d'uso degli strumenti;
- venga rispettata la normativa in tema di privacy;
- lo strumento che "serve" al lavoratore per adempiere la prestazione non venga modificato (per esempio, con l'aggiunta di appositi software di localizzazione o filtraggio) per controllare il lavoratore.

A liberalizzare gli strumenti di controllo degli accessi al lavoro è stato il Jobs Act

che ha riformato l'articolo 4 dello Statuto dei lavoratori. Ora la norma stabilisce che non è necessario né il preventivo accordo coi sindacati, né l'autorizzazione dell'Ispettorato del lavoro per installare strumenti di registrazione degli accessi e delle presenze.

Ma **come avviene il controllo degli accessi a lavoro?** La questione della registrazione delle presenze può porre problemi tutte le volte in cui lo strumento, anziché essere costituito dal consueto cartellino e dalla relativa timbratura, raccoglie invece dati biometrici come l'impronta del dito, la retina, ecc. Sul punto, si devono segnalare alcune pronunce del Garante della Privacy.

Impronta della mano

La rilevazione dell'**impronta della mano** dei lavoratori è ammessa per poter accedere in determinate aree in condizioni di sicurezza, purché:

- non sia costituito alcun archivio;
- i dati siano memorizzati su uno specifico badge e i dati stessi siano cancellati automaticamente dopo 7 giorni.

Dovrà essere comunque garantito un sistema alternativo di accesso (Garante Privacy, provvedimento dicembre 2014).

Dati biometrici dei dipendenti

Con la newsletter n. 473 del 19 febbraio 2021, il Garante per la protezione dei dati personali ha reso noto che è vietato l'utilizzo di un sistema di rilevazione delle presenze basato sul **trattamento di dati biometrici dei dipendenti**, a meno che l'utilizzo sia proporzionato all'obiettivo perseguito, fissando misure appropriate e specifiche per tutelare i diritti degli interessati.

I principali dati biometrici di cui all'intervento sono i seguenti:

- le impronte digitali;
- l'altezza;
- il peso;
- il colore e la dimensione dell'iride;
- la retina;

- la sagoma della mano;
- la forma dell'orecchio oppure la fisionomia del volto.

L'azienda non può quindi acquisire le impronte digitali dei dipendenti memorizzandole in forma crittografata sul badge di ciascun lavoratore per poi verificare l'identità del dipendente stesso mediante il confronto tra il modello biometrico di riferimento, memorizzato all'interno del badge, e l'impronta digitale presentata all'atto del rilevamento della presenza.

Il Garante privacy ha ritenuto che, in questo modo, si effettuava un trattamento di dati biometrici dei dipendenti (sia all'atto dell'emissione del badge, sia all'atto della verifica dell'impronta in occasione di ogni "timbratura" di ciascun dipendente), in assenza di un'idonea base giuridica.

Né il **consenso dei dipendenti**, invocato dall'azienda quale fondamento del trattamento, può essere considerato valido, nel contesto lavorativo, a maggior ragione pubblico, per effetto dello squilibrio del rapporto tra dipendente e datore di lavoro.

Comportamenti di questo tipo non possono essere sdoganati neanche dall'informativa comunicata ai sindacati e ai lavoratori. È necessaria un'apposita comunicazione al Garante della Privacy sul trattamento, per come richiesto dal Regolamento europeo in materia di privacy.

Quando il badge va autorizzato

La Cassazione ha precisato che il badge utilizzato per la rilevazione delle presenze che consente la trasmissione, mediante sistema on line, di tutti i dati acquisiti tramite lettura magnetica, riguardanti non solo l'ingresso e l'uscita, ma anche le sospensioni, i permessi e le pause, così realizzando in concreto un controllo continuo, permanente, globale e a distanza circa l'osservanza da parte degli stessi dipendenti del loro obbligo di diligenza, sotto il profilo dell'orario di lavoro, rientra nella fattispecie di cui all'art. 4, comma 2, L. 300/1970, per cui necessita per essere lecito di un accordo con le rappresentanze sindacali o dell'autorizzazione dell'ispettorato del lavoro **[1]**.

Lo stesso vale per i badge dotati, oltre che del microchip standard, anche del microchip con transponder RFID (identificatore a radio frequenza) che, oltre a

consentire e memorizzare l'accesso e l'uscita dai locali aziendali, è in grado di registrare e memorizzare anche i movimenti del lavoratore all'interno dell'azienda, in funzione del numero e del posizionamento dei sensori installati.

Anche in tal caso, secondo la Cassazione **[2]**, per il suo legittimo utilizzo sarà indispensabile raggiungere un accordo sindacale oppure ottenere l'autorizzazione dell'Ispettorato del lavoro.

Riconoscimento facciale: le linee guida

Nella stessa newsletter n. 473/2021, il Garante privacy ha ricordato che, in data 28 gennaio 2021, nella Giornata europea per la protezione dei dati, il Comitato Consultivo della Convenzione 108, istituito presso il Consiglio d'Europa, ha adottato linee guida in materia di riconoscimento facciale.

Il documento esprime particolare preoccupazione riguardo ai rischi derivanti dal riconoscimento facciale volto a rilevare i tratti della personalità, i sentimenti o le reazioni emotive dall'immagine del volto: le cosiddette tecnologie di "riconoscimento dell'affetto". Tali tecnologie – afferma il Comitato – dovrebbero essere vietate e non dovrebbero essere impiegate, ad esempio, nelle procedure di assunzione di personale, nell'accesso ai servizi assicurativi e all'istruzione.

Allo stesso modo, non dovrebbe essere consentito l'uso del riconoscimento facciale al solo scopo di determinare il colore della pelle di una persona, le convinzioni religiose o di altro tipo, il sesso, l'origine etnica, l'età, le condizioni di salute o le condizioni sociali.

Le aziende e le pubbliche amministrazioni che intendano avvalersi di tecniche di riconoscimento facciale, da parte loro, hanno l'obbligo di garantire il rispetto dei principi di protezione dati, compresa la necessità di effettuare una valutazione dei rischi che il ricorso a tali tecniche può avere sui diritti delle persone, nonché dei profili etici che ne derivano, anche attraverso l'ausilio di comitati di esperti indipendenti.