l'officina dei numeri

circolare informativa n. 7/2022 del 18 maggio 2022
Studio Associato Picchio e Gorretta, via Fausto Coppi 3 – 15121 – Alessandria
tel. e fax 0131 443273 – 0131 267858 e-mail: info@picgor.it - sito web: www.picgor.it

BADGE AZIENDALE E APP DI RILEVAZIONE PRESENZE: AMMISSIBILITÀ E CONDIZIONI D'USO

a cura di Francesca Cuzzetto

PREMESSA

In continuità con il tema di tutela della riservatezza dei dati personali, del quale la circolare 4/2022 ("*La geolocalizzazione: ammissibilità dei controlli satellitari e sue condizioni*") ha svolto la funzione di "apri pista", con la presente trattazione ci si propone di illustrare i profili di ammissibilità dei controlli datoriali da effettuarsi tramite badge aziendale nonché, da ultimo - in quanto trattasi di uno strumento di più recente acquisizione - per mezzo di *app* su dispositivi mobili geolocalizzabili, ambedue strumenti destinati alla rilevazione delle presenze sul luogo di lavoro.
Di seguito si procederà all'esame di alcune interessanti pronunce giurisprudenziali e provvedimenti del Garante della privacy, nei quali i frequenti richiami normativi saranno rivolti al D.Lgs. 196/2003 (cd. "Codice della privacy"), al D.Lgs. 101/2018 (in attuazione del reg. UE 2016/679, cd. GDPR) nonché all'art. 4 legge 300/1970 (cd. "Statuto dei lavoratori").

IL VALORE D'USO DEL BADGE E LA NORMATIVA DI RIFERIMENTO: L'ARTICOLO 4 DELLO STATUTO DEI LAVORATORI.

L'utilizzo del badge aziendale, per essere coerente con lo scopo perseguito dal legislatore, deve potersi conformare all'art. 4, comma 2 della legge 300/1970 (non presente nel testo originario della norma ma aggiunto a far data dal 2015) che recita: "*La disposizione di cui al comma 1* [che prevede l'obbligo di accordo sindacale o di autorizzazione preventiva dell'ispettorato del lavoro per installare impianti audiovisivi o altri mezzi di controllo a distanza dei lavoratori] *non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze*".
Diversamente,ogni qualvolta il datore di lavoro intenda adoperare il badge elettronico insieme ad altri strumenti - dalla cui combinazione sia possibile ricavare informazioni eccedenti rispetto a quelle sufficienti a rilevare la mera presenza del lavoratore sul luogo di lavoro - tale impiego di mezzi, per potersi considerare lecito, e dunque idoneo al raggiungimento dello scopo perseguito, dovrà essere preceduto da un accordo sindacale aziendale con le RSA o RSU (o dalle Oo.Ss. in presenza di più unità produttive) motivato "*esclusivamente* [da] *esigenze organizzative e produttive,* [dal]*la sicurezza del lavoro e* [dal]*la tutela del patrimonio aziendale"* o, in assenza di dette rappresentanze, essere autorizzato preventivamente dal competente ispettorato del lavoro per le medesime finalità.
Poiché le informazioni, pur raccolte legittimamente dal datore di lavoro in forza di accordo collettivo o di autorizzazione della pubblica autorità, in forza della stretta connessione con gli strumenti di lavoro, presuppongono un'invasione dello spazio di riservatezza del lavoratore, il comma 3 dell'art. 4 cit. dispone "*che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli nel rispetto di quanto disposto dal Decreto legislativo 196/2003*".

L'USO IMPROPRIO DEL BADGE E LA NECESSARIA AUTORIZZAZIONE

Nel caso deciso dalla sentenza della Corte di Cassazione 15892/2007, la società ricorrente, come emerge dalle pronunce di merito e dalle stesse difese delle parti, al fine di agevolare i propri dipendenti muniti di autovettura, aveva predisposto per essi un garage ove posteggiarla durante l'orario lavorativo, inserendo tuttavia un congegno di sicurezza volto a consentire l'ingresso a tale garage solo attraverso il badge elettronico personale assegnato a ciascun dipendente, già preposto ad attivare gli ingressi agli uffici.
Oltre a consentire l'innalzamento della sbarra di ingresso/uscita dal garage, il congegno identificava e registrava coloro che transitavano nell'area di interesse. Incrociando i dati così ottenuti con quelli rilevati all'ingresso degli uffici, la società era entrata in possesso delle informazioni comprovanti gli inadempimenti posti in essere da un lavoratore, poi licenziato per giusta causa, consistenti in frequenti e immotivati allontanamenti dal posto di lavoro.
Contro il provvedimento datoriale agiva in giudizio il lavoratore, ottenendo l'accoglimento della domanda da parte del tribunale, il quale motivava l'annullamento del licenziamento con l'inesistenza dell'accordo sindacale o dell'autorizzazione dell'ispettorato, elemento necessario a legittimare l'installazione e il successivo utilizzo di apparecchiature che consentano di effettuare controlli a distanza sull'attività lavorativa.
Il datore di lavoro, impugnata la pronuncia, si rivolgeva alla Corte d'appello la quale, non ritenendo i controlli denunciati dall'appellato eccessivamente invasivi ed illeciti bensì, al contrario, idonei ad accertare gli atti che ne hanno determinato il licenziamento, accoglieva l'appello, dichiarando la legittimità del recesso.
Avverso tale sentenza il lavoratore ricorreva in Cassazione denunciando - per ciò che qui interessa - la violazione e falsa applicazione dell'art. 4 della legge 300/1970, ritenendo che il controllo eseguito avesse comportato l'accesso ad una quantità di informazioni eccedenti rispetto a quelle che sarebbero state sufficienti al perseguimento del fine dichiarato dal datore di lavoro - ovvero quello di garantire la custodia delle

auto – in assenza del previsto accordo o della autorizzazione preventiva.
La Corte di Cassazione, non potendo effettuare alcun bilanciamento tra i contrapposti interessi delle parti, precluso - a priori - dall'inadempimento delle formalità prescritte dalla legge, si pronunciava in favore del lavoratore, cassando la pronuncia impugnata.
La Corte, pur non disconoscendo l'antigiuridicità della condotta del lavoratore, di per sé astrattamente idonea a giustificare il licenziamento, ritiene che le informazioni raccolte, in quanto le stesse, pur pacifiche, non sono utilizzabili ai fini della prova, non essendo state ottenute con l'utilizzo di sistemi di controllo a distanza legittimamente installati e utilizzati, con il corretto adempimento delle condizioni previste dalla norma.
L'accordo sindacale o l'autorizzazione preventiva, sempre necessari quando gli strumenti oggetto di controllo siano altro dal *badge* utilizzato per rilevare le presenze in azienda o dagli strumenti strettamente necessari allo svolgimento della prestazione, deve dunque ritenersi indispensabile anche in quelle situazioni, come nel caso in esame, in cui il *badge* venga impiegato per fini diversi o in combinazione con altri mezzi, e che pertanto si appresti a rilevare e trattare un maggior numero di dati di quelli consentiti in assenza di accordo o autorizzazione.
Nel determinare le condizioni di ammissibilità dei controlli a distanza da effettuarsi sul posto di lavoro il legislatore - condizionando l'utilizzo di impianti, apparecchiature e sistemi di sorveglianza all'esistenza di comprovate esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, secondo la richiamata sentenza - ha attribuito a tali fattispecie il carattere della tassatività, escludendo perciò la possibilità di ricomprendere tra i beni protetti da controlli difensivi quelli personali dei lavoratori, che non avendo alcun legame con l'attività produttiva dell'azienda non possono esservi sottoposti.
Pertanto, il tentativo del datore di lavoro di motivare la legittimità dell'utilizzo delle informazioni acquisite con la finalità di tutelare anche i beni di terzi (propri dipendenti) non trova l'assenso della Corte laddove tale garanzia di sicurezza comporti un costo troppo alto per il lavoratore, che in ragione di tale sorveglianza, si trova a poter disporre di un limitato spazio di riservatezza.

LA SORVEGLIANZA SULLE PRESENZE ED I LIMITI DI AMMISSIBILITÀ

Similmente alla situazione dianzi riportata, la decisione della Corte di Cassazione 9904/2016 è relativa ad un ricorso del datore di lavoro avverso una sentenza del giudice di merito in ordine alla declaratoria di illegittimità di un licenziamento disposto nei confronti di un proprio collaboratore.
Dai fatti riportati in giudizio, risulta che il datore di lavoro avesse licenziato il lavoratore dopo averne rilevato una presenza fittizia sul luogo di lavoro, resa possibile da un collega che effettuava le timbrature in ingresso e in uscita dalla sede di lavoro, in sua vece.
Nella pacifica risultanza del fatto, la controversia si fondava sulla contestazione dei mezzi utilizzati ai fini della prova. Infatti, il *badge* in uso ai dipendenti, essendo dotato di un meccanismo di rilevazione, comparazione e registrazione di dati incorporati, risultava idoneo ad essere qualificato come mezzo di controllo a distanza, e perciò inammissibile come strumento di prova, in difetto di accordo sindacale o di autorizzazione preventiva.
A determinare la pronuncia di illegittimità del licenziamento impugnato concorre la disposizione dell'art. 4 della legge 300/1970 che - come si è osservato - ammette l'applicazione diretta, ovvero senza accordo sindacale o autorizzazione preventiva, solo laddove gli strumenti di registrazione degli accessi e delle presenze, siano impiegati secondo gli usi che sono loro propri e non in combinazione con altri strumenti che consentano di ampliare il controllo sui lavoratori oltre il limite consentito.
Il collegio giudicante, nel dare priorità al rispetto della forma sulla sostanza, ovvero nel rigettare le istanze probatorie che non siano conformi alle procedure previste dalla legge, si fa pertanto portavoce delle insopprimibili garanzie processuali di certezza e di tutela.

RECESSO LEGITTIMO PER ESPRESSA AMMISSIONE DI COLPA

Nella controversia decisa dalla Corte d'Appello di Venezia con la sentenza 439/2019, una lavoratrice si opponeva al licenziamento intimatole per giustificato motivo soggettivo; secondo la contestazione disciplinare mossale, la stessa sarebbe stata vista da una collega, più di una volta, mentre rientrava in ufficio dopo la pausa pranzo, senza effettuare la timbratura che - da regolamento aziendale - precede il rientro in servizio, e che pertanto, deve coincidere con il termine della pausa pranzo dell'interessato. La stessa, seguendola, avrebbe poi scoperto che l'appellante aveva effettuato le timbrature indicanti l'inizio e il termine della pausa pranzo nel medesimo istante, senza che il periodo di tempo intercorrente tra questi due momenti fosse effettivamente trascorso.
Il datore di lavoro, messo a parte dell'avvenimento dalla testimone oculare, avrebbe poi dato seguito ad una serie di accertamenti con l'intento di verificare i fatti riportati: dal raffronto effettuato tra gli orari delle timbrature e quelli di acquisto di vivande alla mensa aziendale (transazione che veniva effettuata con il medesimo *badge* ed era quindi puntualmente registrata e tracciata), è stato possibile appurare la ripetitività delle azioni fraudolente poste in essere dalla lavoratrice.
L'appellante lamentava in proposito un'invasione ingiustificata del proprio spazio di riservatezza, opponendosi pertanto a che la società datrice di lavoro potesse introdurre in giudizio informazioni eccedenti rispetto a quelle che siano state recepite con il consenso della lavoratrice stessa (e riguardanti l'utilizzo del *badge* esclusivamente come strumento di rilevazione delle presenze).
La lavoratrice, in particolare, chiedeva che venisse dichiarata l'illegittimità delle prove raccolte in violazione dell'art. 13 del D. Lgs. 196/2003 (in allora vigente), in quanto il datore di lavoro non avrebbe fornito l'informativa necessaria, non mettendola – pertanto - nelle condizioni di prevedere né la tipologia di dati ai quali la società avrebbe potuto accedere, né l'uso al quale gli

stessi sarebbero stati destinati o i tempi di conservazione presso l'azienda.
La Corte pur condividendo l'assunto per cui si dovessero espungere le prove addotte in violazione del citato art. 13, rigettava comunque la domanda della lavoratrice sulla base delle affermazioni rilasciate dalla stessa in corso di giudizio, nelle quali ammetteva di aver commesso gli atti e le infrazioni a lei imputate, fornendo essa stessa la prova degli inadempimenti contestati (prova altrimenti non raggiungibile con le produzioni datoriali non ritenute ammissibili).

LEGITTIMITÀ E LIMITI DELLA APP DI RILEVAZIONE DELLE PRESENZE: PROVVEDIMENTO DEL GARANTE N. 350 DEL 8.9.2016

Due società intendendo sostituire quantomeno parzialmente i mezzi di rilevazione delle presenze tradizionali impiegati in azienda (foglio delle presenze e *badge* elettronico), si rivolgono al Garante della Privacy affinché verifichi la sussistenza delle condizioni e dia la propria approvazione a che le stesse possano lecitamente richiedere ai dipendenti (che posseggano uno *smartphone* e che esprimano il proprio assenso) di installare su tale dispositivo una specifica applicazione contenente una funzionalità di localizzazione geografica, preordinata all'esecuzione della "timbratura del cartellino e della rilevazione presenze" nonché, ove prevista, della pausa pranzo, tramite l'inserimento delle credenziali di accesso del singolo lavoratore.
Con l'utilizzo di tale strumento le richiedenti intendono soddisfare le proprie esigenze di riduzione del tempo di rilevazione delle presenze, di risparmio sui costi di gestione dei badge, di rilevazione con un maggior grado di certezza dell'effettiva presenza del collaboratore sul luogo di lavoro, nonché di ottimizzazione della gestione degli infortuni sul lavoro.
Lo strumento proposto si presenta adatto ad essere applicato a tutti i lavoratori e, in particolar modo, a coloro che svolgono la propria mansione al di fuori della sede aziendale o in missione presso i clienti.
Ai suddetti lavoratori verranno fornite le necessarie informazioni volte a stabilire:

- le modalità e le finalità d'uso del dispositivo
- l'identità dei responsabili o degli incaricati al trattamento dei dati personali;
- i dati personali trattati attraverso l'installazione sui dispositivi (identificativo del dipendente, orario di entrata, luogo di timbratura, orario di uscita dispositivo tramite il quale viene effettuata la timbratura) e la designazione del soggetto responsabile o incaricato al trattamento;
- i tempi di conservazione delle informazioni ottenute;
- l'esclusione della capacità del mezzo di operare un controllo sull'attività lavorativa degli utilizzatori, nonché il tracciamento costante degli spostamenti effettuati dal collaboratore;
- i mezzi per prevenire un collegamento continuo e inconsapevole al dispositivo e per impedire il trattamento (anche incidentale) dei dati collegati all'uso del cellulare, ma estranei alle finalità perseguite dalla *app*;

Il Garante accoglie la domanda e prescrive alle società di:

- cancellare il dato relativo alla posizione del lavoratore non appena abbia verificato la corrispondenza tra le coordinate geografiche della sede di lavoro e la posizione del lavoratore;
- configurare il sistema in modo tale che sul dispositivo sia posizionata un'icona che indichi che la funzionalità di localizzazione è attiva;
- adottare specifiche misure idonee a garantire che il dispositivo installato non possa effettuare trattamento di dati ultronei (ad es. dati relativi al traffico telefonico, agli SMS, alla posta elettronica, alla navigazione su *internet*, ecc.);

Con riguardo all'espletamento delle formalità prescritte ai fini di un lecito impiego dello strumento, il Garante si rivolge ancora alle società rammentandole di:

- ➔ effettuare la notifica preventiva ai sensi dell'art. 37, comma 1, lett. a) del Codice della Privacy (adempimento oggi abrogato, per cui la richiesta di autorizzazione preventiva è limitata a casi particolari, nei quali in esito alla valutazione dei rischi operata emerga che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuarlo);
- ➔ fornire ai dipendenti un'informativa completa di tutti gli elementi di cui all'art. 13 del Reg. UE 679/2016;
- ➔ effettuare la designazione di incaricati e responsabili del trattamento dei dati;
- ➔ adottare le misure di sicurezza previste dagli artt. 32 e ss. del Reg. UE 679/2016;
- ➔ predisporre misure al fine di dare all'interessato la conferma che sia in corso un trattamento dei dati personali che lo riguardano (in sostanza si tratta di un *alert* che avvisi quando la geolocalizzazione è attiva.