Dal badge ai sistemi di rilevazione antropobiometrici

Controllo accessi e presenze: condizioni di legittimità

Massimo Tommaso Goffredo e Vincenzo Meleca

Con la modifica dell'articolo 4, legge n. 300/1970 attuata con l'articolo 23, comma 1, D.Lgs. n. 151/2015, il legislatore, alla luce dei mutamenti organizzativi apportati dall'uso delle tecnologie telematiche (personal computers, tablets, smartphone, badge, ecc.) ha cercato di aggiornare le modalità per il loro uso legittimo, chiarendo in particolare che la necessità di un preventivo accordo sindacale (o, in mancanza di questo, della preventiva autorizzazione dell'Ispettorato del lavoro) non sussiste per "*gli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze*".

L'unico onere che incombe sul datore di lavoro è quello di fornire 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*".

Ottemperato correttamente a tale onere, il datore di lavoro dovrebbe così poter effettuare su detti strumenti tutti i controlli che ritiene opportuni, utilizzando le informazioni così raccolte "*a tutti i fini connessi al rapporto di lavoro*", evidentemente comprese le sanzioni disciplinari.

Sin dalla stesura del disegno di legge, diventato poi il D.Lgs. n. 151/2015, si erano però levate una serie di voci critiche, sia da parte di alcune organizzazioni sindacali, Cgil in testa, sia anche da parte del Garante della privacy (1). A proposito di quest'ultimo, va evidenziata una sorta di diffidenza verso le nuove tecnologie, tanto che, almeno in un'occasione, l'Autorità ha ritenuto di dover affermare che "*con riferimento all'uso di tecnologie biometriche per finalità di rilevazione delle presenze si osserva che la legittima finalità volta ad accertare il rispetto dell'orario di lavoro anche 'mediante forme di controlli obiettivi e di tipo automatizzato (e in taluni casi a garantire speciali livelli di sicurezza)' deve, in ogni caso, essere effettuato nel pieno rispetto della disciplina in materia di protezione dei dati personali, anzitutto con riguardo all'osservanza dei principi di necessità e proporzionalità ... secondo cui 'il datore di lavoro è sempre tenuto a cercare i mezzi meno invasivi scegliendo, se possibile, un procedimento non biometrico'. Tali principi impongono che siano preventivamente considerati altri sistemi, dispositivi e misure di sicurezza fisiche e logicistiche* (sic) *che possano assicurare parimenti una puntuale e attendibile verifica delle presenze e degli ingressi sul luogo di lavoro senza fare ricorso al trattamento dei dati biometrici*" (2). Così trascurando la funzione essenziale di tali sistemi che è quella di garantire una maggiore sicurezza e minori adempimenti amministrativi.

La cornice normativa

Prima di accennare a quelle che sono le norme di legge fondamentali di riferimento specifico al potere datoriale di controllo su accessi e presenze, occorre citare due norme di legge a carattere più generale, contenute nel Codice civile, gli articoli. 2086 e 2087, che stabiliscono, il primo, il potere organizzativo del datore di lavoro ("*L'imprenditore è il capo dell'impresa*") ed, il secondo, i suoi doveri nei confronti dei suoi dipendenti ("*... è tenuto ad adottare ... le misure ... necessarie a tutelare l'integrità fisica e la personalità morale dei prestatori di lavoro*)". Passando dun-

(1) Cfr. L'intervento di Antonello Soro, Presidente del Garante per la protezione dei dati personali, sul quotidiano *L'Huffington Post*, 8 settembre 2015, riportato anche sul sito del garante Privacy.

(2) Cfr. Provvedimento n. 357 del 15 settembre 2016, Verifica preliminare. Sistema di lettura di dati biometrici mediante parziale identificazione dell'impronta digitale per la rilevazione della presenza in servizio.

que alle norme specifiche, queste sono l'articolo 4, legge n. 300/1970 (c.d. Statuto dei lavoratori") e l'articolo 114, D.Lgs. n. 196/2003 (c.d. "Codice della privacy"). Ad esse vanno aggiunti anche gli articoli 13, commi 4 e 5 e 24, comma 1, lettere *a*), *b*), *e*), *f*), citato D.Lgs. n. 196/2003.
Oltre alle citate norme di legge vanno inoltre tenuti presenti alcuni provvedimenti del Garante della Privacy, quali le linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro del 14 giugno 2007 ed alcuni tra i più recenti provvedimenti quali, ad esempio, quelli del 16 marzo 2017 (3), del 16 febbraio 2017, 15 settembre 2016 e 15 marzo 2016 (4), nonché quello dell'8 settembre 2016 (5).

Destinatari delle norme in materia di controllo accessi

Sono soggetti al rispetto delle norme di legge in materia di controllo accessi e presenze tutti i datori di lavoro pubblici e privati, di qualsiasi settore merceologico e di qualsiasi dimensione. I datori di lavoro, in funzione di tali obblighi, ma anche del loro potere organizzativo, riconosciuto dall'art. 2086 c.c., hanno il diritto di fissare, unilateralmente oppure con accordo sindacale, delle regole per l'accesso ai locali aziendali e per la verifica della presenza negli stessi di chiunque, ed in particolare:
• dei propri lavoratori subordinati (o a questi assimilati, come i lavoratori somministrati);
• dei lavoratori autonomi e di quelli dipendenti da altri datori di lavoro (come quelli distaccati o in appalto) che debbano svolgere la loro attività all'interno di detti locali aziendali;
• dei terzi (clienti, fornitori, visitatori).
Tutte queste persone hanno, di conseguenza, l'obbligo di attenersi alle regole fissate dai datori di lavoro.

Tipologia degli strumenti di registrazione degli accessi e delle presenze

L'accesso di persone, siano esse lavoratori o terzi, ai locali aziendali e la loro presenza negli stessi costituiscono aspetti importanti sotto vari punti di vista, legati:
• alla sicurezza, intesa come tutela del patrimonio aziendale (security);
• alla sicurezza del lavoro (safety);
• all'obbligo di calcolare l'orario di lavoro ai fini retributivi;
• al rispetto dei limiti previsti dalla legge e dalla contrattazione collettiva in materia di orario di lavoro;
• al rispetto delle normative aziendali in materia di orario di lavoro, ai fini disciplinari.
In passato (ma ancora oggi nelle microaziende) la registrazione degli accessi e delle presenze, quando veniva effettuata, si basava sul cosiddetto "registro presenze" (gestito spesso dall'addetto alla portineria) o sul cosiddetto "libro firma" (sul quale ogni persona apponeva la propria firma, indicando gli orari della propria entrata ed uscita dal sito aziendale). Tali supporti cartacei furono poi sostituiti dai cosiddetti "cartellini-orologio", che ogni dipendente doveva timbrare in appositi orologi "marcatempo" ogni qualvolta entrava od usciva dal sito aziendale (in molti casi, anche quando sospendeva l'attività lavorativa, come ad esempio per la pausa-pasto).
Il controllo degli accessi veniva fatto, laddove presente, anche visivamente dal personale di vigilanza, mentre il controllo della presenza, oltre che visivamente dal diretto responsabile del lavoratore, poteva venir effettuato da persona della Direzione delle Risorse Umane.
Da almeno un paio di decenni, la tecnologia ha sostituito in gran parte l'attività umana appena descritta, consentendo all'azienda, in tempo reale, di sapere non solo chi è entrato e chi è uscito ed in quali orari, ma anche di sapere dove il lavoratore (o il terzo) si trovi esattamente.
Nelle note seguenti descriveremo i principali tra questi strumenti tecnologici e le condizioni di legittimità per il loro uso:
• badge;
• smartphone;
• sistemi di rilevazione antropobiometrici (impronte digitali, scansione dell'iride o della retina, biometria facciale).

(3) Nel primo provvedimento il badge avrebbe dovuto essere utilizzato a bordo di veicoli aziendali dotati di appositi lettori.
(4) Questi provvedimenti affrontano il problema del controllo delle presenze ed accessi effettuato, in aggiunta al badge, anche con altri sistemi, quali la rilevazione biometrica facciale (il primo) e la rilevazione di impronte digitali (gli altri).
(5) Nel provvedimento si affronta il problema della sostituzione del badge con altri sistemi, quali l'utilizzo di smartphone.

Badge

Con questo termine anglosassone si indicano delle tessere, normalmente delle dimensioni di una carta di credito, che possono essere munite di banda magnetica o di altri dispositivi, quali ad esempio microchip (componenti elettronici integrabili con altri sistemi similari), Rfid (acronimo che sta per Radio-Frequency IDentification, in italiano Identificazione a Radiofrequenza), per l'utilizzo con apparecchiature informatiche ed elettroniche. Queste tessere possono riportare in chiaro informazioni personali (fotografie, nominativo, data di nascita e altre indicazioni utili allo scopo per cui sono utilizzati) e memorizzare nella banda magnetica o nel microchip varie altre informazioni. In funzione dello scopo per cui sono stati prodotti, possono consentire al lavoratore dipendente dal datore di lavoro titolare o fruitore dei locali aziendali:

• il solo accesso ai locali aziendali, con successiva uscita dagli stessi, senza alcun tipo di interazione con i sistemi informativi aziendali. In buona sostanza, questo tipo di badge altro non è se non il sostituto della normale chiave. Per il loro uso non è richiesto alcun tipo di procedura (6);

• se il badge ha la banda magnetica o il microchip, accesso ai - e uscita dai - locali aziendali, con memorizzazione dei relativi orari da parte del sistema informativo aziendale. In base all'art. 4, legge n. 300/1970, come modificato dal D.Lgs. n. 151/2015, per il loro uso legittimo è richiesto al datore di lavoro di fornire al lavoratore adeguata informazione sulle sue modalità d'uso e sulle modalità di effettuazione dei controlli, nel rispetto di quanto disposto dal D.Lgs. n. 196/2003 sulla privacy. Le informazioni raccolte tramite sistema informativo sono utilizzabili dal datore di lavoro per tutti i fini connessi al rapporto di lavoro, ivi comprese le eventuali sanzioni disciplinari, come in caso di mancato rispetto del loro uso (ad esempio se è stato previsto che debbano essere indossati in modo da essere visibili) o di mancato rispetto dell'orario di lavoro (ad esempio, per ritardi o uscite anticipate non autorizzate);

• se il badge ha particolari e specifici microchip o bande magnetiche (oppure è necessario utilizzare un codice alfanumerico) e consente, oltre all'accesso ai - e uscita dai - locali aziendali, anche l'accesso a - e uscita da - specifici locali aziendali (in genere riservati, come ad esempio uffici di ricerca e sperimentazione, caveau bancari ecc.), con memorizzazione dei relativi orari da parte del sistema informativo aziendale, per il suo legittimo utilizzo sarà indispensabile raggiungere un accordo sindacale oppure ottenere l'autorizzazione dell'Ispettorato del lavoro;

• se il badge ha, oltre al microchip standard, anche un microchip con transponder Rfid (7) che, oltre a consentire e memorizzare l'accesso ai - 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, per il suo legittimo utilizzo sarà indispensabile raggiungere un accordo sindacale oppure ottenere l'autorizzazione dell'Ispettorato del lavoro.

Per il personale viaggiante (in particolare per i conduttori di autoveicoli da trasporto persone o materiali) si è posto il problema di appositi terminali installati sugli autoveicoli, utilizzabili anche come lettori di badge ai fini della rilevazione presenze. Per il Garante della Privacy, se tali sistemi consentono anche di rilevare gli spostamenti del veicolo, le pause, i tempi di carico e scarico, la distanza percorsa, i tempi di percorrenza e la velocità media, per il loro legittimo utilizzo sarà indispensabile raggiungere un accordo sindacale oppure ottenere l'autorizzazione dell'Ispettorato del lavoro (8).

Smartphone

In questi telefoni cellulari "intelligenti" è possibile inserire un'applicazione, attivata dal lavoratore al momento in cui accede al sito lavorativo o ne esce, che consente di acquisire informazioni da remoto per controllo accessi e presenze, evi-

(6) Non può essere considerata badge per l'accesso ai locali aziendali o per la verifica della presenza negli stessi la tessera di riconoscimento dei dipendenti delle imprese in appalto, contenente, ai sensi dell'art. 26, comma 8, D.Lgs. n. 81/2008, la fotografia e le generalità del lavoratore e l'indicazione del suo datore di lavoro.

(7) In genere, il microchip è di tipo passivo, cioè privo di alimentazione elettrica. Al passaggio nei pressi di un lettore, questo emette un segnale radio a frequenze basse o medie che attiva il microchip e gli fornisce l'energia necessaria a rispondere al lettore, ritrasmettendogli un segnale contenente le informazioni memorizzate nel chip stesso.

(8) Cfr. Provvedimento n. 138 del 16 marzo 2017, "Trattamento di dati personali di dipendenti effettuato attraverso la localizzazione di veicoli aziendali".

tando così di doversi dotare di terminali con lettore optronico e di relativi badge (9). Se lo smartphone è di proprietà aziendale ed è stato affidato al lavoratore come strumento di lavoro, magari anche con possibilità di uso personale, per il suo legittimo controllo da parte del datore di lavoro, secondo il Garante della Privacy (10) non è sufficiente fornire al lavoratore adeguata informazione sulle sue modalità d'uso e sulle modalità di effettuazione dei controlli, ma il datore di lavoro deve anche provvedere a:

• cancellare il dato relativo alla posizione del lavoratore, avendo verificato preventivamente l'associazione tra le coordinate geografiche della sede di lavoro e la posizione del lavoratore, conservando, eventualmente, il solo dato concernente la predetta sede di lavoro, alla data e all'orario cui si riferisce la timbratura;

• 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 l'applicativo installato sul dispositivo del dipendente non possa effettuare trattamenti di dati ultronei (es. dati relativi al traffico telefonico, agli sms, alla posta elettronica o alla navigazione in internet o altro).

Soltanto avendo adempiuto questi oneri, lo stesso datore di lavoro potrà utilizzare le informazioni raccolte e memorizzate dal sistema informativo aziendale per tutti i fini connessi al rapporto di lavoro, ivi comprese le eventuali sanzioni disciplinari, come in caso di mancato rispetto del loro uso (ad esempio se è stato previsto che debbano essere indossati in modo da essere visibili) o di mancato rispetto dell'orario di lavoro (ad esempio, per ritardi o uscite anticipate non autorizzate);

Sulla scorta di questa posizione del Garante riteniamo che il datore di lavoro, ove ritenga di dover effettuare altri controlli oltre quelli relativi all'accesso ai locali aziendali ed alla presenza negli stessi, debba necessariamente ottenere un accordo con le rappresentanze sindacali aziendali o l'autorizzazione dell'Ispettorato del lavoro.

Sistemi di rilevazione antropobiometrici

Questi sistemi per il controllo degli accessi ai locali aziendali (attualmente vengono utilizzati quelli per la rilevazione di impronte digitali o palmari oppure per il riconoscimento della retina o dell'iride. Ancora raramente quelli per la rilevazione di elementi di biometria facciale) sono basati su apparecchiature (scanner) che confrontano immagini elettroniche degli elementi antropobiometrici sopra indicati (11) e precedentemente memorizzati, con quelle rilevate al momento in cui il lavoratore accede ai locali aziendali o ne esce.

Le informazioni così raccolte vengono trasferite automaticamente al sistema informativo aziendale sia per la rilevazione delle presenze, sia per motivi di sicurezza del lavoro, sia infine per motivi di semplice identificazione del lavoratore.

In assenza di specifiche norme di legge, la disciplina di tali sistemi è demandata principalmente al Garante della Privacy, il quale, come già accennato in premessa, ha comunque espresso forti perplessità in merito all'utilizzo di sistemi antropobiometrici per la rilevazione della presenza in servizio (12).

Sistemi di lettura di dati biometrici mediante identificazione dell'impronta digitale

Premesso che per il Garante della Privacy "*il datore di lavoro è sempre tenuto a cercare i mezzi meno invasivi scegliendo, se possibile, un proce-*

(9) In alternativa, lo smartphone può essere utilizzato come badge, avvicinandolo agli appositi terminali. La distanza di lettura è regolabile da 30 cm fino a 10 metri. Questa versatilità rende possibile diverse applicazioni: dalla rilevazione presenze e controllo accessi agli uffici (distanza di lettura di qualche cm) o ad altre aree, quali ad esempio controllo accessi a parcheggi riservati con attivazione dalla propria auto (distanza di lettura di qualche metro).

(10) Cfr. Provvedimento n. 350 dell'8 settembre 2016 "Verifica preliminare. Trattamento di dati personali dei dipendenti effettuato attraverso la localizzazione di dispositivi smartphone per finalità di rilevazione delle presenze".

(11) Allo stato degli atti i sistemi di rilevazione antropobiometrici prendono in considerazione quattro tipi di parametri fondamentali: la dattiloscopia, la geometria della mano, alcuni componenti dell'apparato visivo, la biometria facciale. Cfr. Nello Balossino e Simona Siracusa, *L'identificazione basata sul volto: metodi fisionomici e metrici*, Security Forum 2004.

(12) Sull'utilizzo di sistemi di rilevazione biometrica per il riconoscimento biometrico, installati su macchinari allo scopo di impedire il loro utilizzo da parte di soggetti non autorizzati, l'Ispettorato Nazionale del Lavoro, con circolare n. 5 del 19 febbraio 2018 ha affermato che esso può essere considerato uno strumento indispensabile a "*... rendere la prestazione lavorativa ... e pertanto si possa prescindere, ai sensi del comma 2, art. 4 della legge n. 300/1970, sia dall'accordo con le rappresentanze sindacali sia dal procedimento amministrativo di carattere autorizzativo previsto dalla legge*". Riteniamo che tale orientamento possa estendersi anche ai sistemi di rilevazione antropobiometrici utilizzati per il controllo accessi e presenze.

dimento non biometrico" e che i principi generali di tutela dei dati personali *"impongono che siano preventivamente considerati altri sistemi, dispositivi e misure di sicurezza fisiche e logicistiche (sic) che possano assicurare parimenti una puntuale e attendibile verifica delle presenze e degli ingressi sul luogo di lavoro senza fare ricorso al trattamento dei dati biometrici*", in base alle più recenti posizioni espresse dal Garante, per la legittimità del loro uso il datore di lavoro dovrà:
• effettuare la notificazione al Garante; fornire ai dipendenti coinvolti dai descritti trattamenti, un'informativa comprensiva di tutti gli elementi indicati dall'art. 13, D.Lgs. n. 196/2003 (tipologia di dati, finalità e modalità del trattamento), compresi i tempi di conservazione;
• adottare le misure di sicurezza necessarie a preservare l'integrità dei dati trattati e prevenire l'accesso agli stessi da parte di soggetti non autorizzati;
• predisporre tutte le misure per garantire agli interessati l'esercizio dei diritti previsti dal citato D.Lgs. n. 196/2003.
Se i dati raccolti con tali sistemi si limitano al controllo accessi e presenze, riteniamo non si debba ottenere un accordo con le rappresentanze sindacali aziendali o l'autorizzazione dell'Ispettorato del lavoro (13).

Sistemi di rilevazione e comparazione della biometria facciale

Fermo restando quanto sopra detto a proposito della posizione alquanto contraria del Garante Privacy circa l'impiego di sistemi di controllo mediante uso di sistemi antropobiometrici, circa quelli basati sulla rilevazione e comparazione della biometria facciale, lo stesso Garante ne ha ritenuta legittima la loro utilizzazione in particolare a condizione che:
• tutti i soggetti che effettueranno le operazioni di trattamento (con particolare riguardo alla raccolta dei dati durante la fase di enrollement) quali incaricati o, eventualmente, responsabili siano designati per iscritto, impartendo loro idonee istruzioni alle quali attenersi;
• l'accesso ai dati e al sistema sia consentito ai soli soggetti incaricati, muniti di specifiche credenziali o dispositivi di autenticazione;
• gli accessi ai dati siano tracciati e le registrazioni comprendano i riferimenti temporali ed abbiano caratteristiche di completezza, integrità, inalterabilità e durata della conservazione analoghe a quelle richieste per i log degli accessi degli amministratori di sistema;
• il sistema di controllo accessi, costituito dai dispositivi di acquisizione, dai lettori e dal server, deve utilizzare una Lan o Vlan dedicata, e deve essere separato dagli altri sistemi che trattano dati personali dei dipendenti per altre finalità;
• la funzione di configurazione del sistema che consente di conservare nei log le immagini relative agli eventi registrati sia disattivata. (14)

Note conclusive

Anche in base agli orientamenti giurisprudenziali più recenti, possiamo affermare che:

(13) Cfr. Provvedimento n. 357 del 15 settembre 2016, "Verifica preliminare. Sistema di lettura di dati biometrici mediante parziale identificazione dell'impronta digitale per la rilevazione della presenza in servizio". Con il Provvedimento n. 129 del 17 marzo 2016, "Sistema biometrico basato sul trattamento di impronte digitali per finalità di rilevazione delle presenze dei dipendenti di un Comune", il Garante aveva ritenuto illegittimo l'uso sia per motivi procedurali (mancata notifica al Garante) sia per il fatto che non era stata fornita un'adeguata informativa ai dipendenti stessi né era stato raccolto il loro consenso. In precedenza il Garante aveva ritenuto illegittimo l'uso della rilevazione di impronte digitali per il controllo accessi e presenze sia con Provvedimento n. 552 del 22 ottobre 2015, "*Rilevazione delle presenze dei dipendenti di un Comune tramite un sistema biometrico basato sul trattamento di impronte digitali*", in quanto *"Le circostanze rappresentate dal Comune non sono idonee a soddisfare i principi di necessità e proporzionalità (in relazione alla finalità perseguita) dei trattamenti effettuati (artt. 3 e 11, Codice). Il Comune infatti non ha indicato specifiche e concrete ragioni in base alle quali altri e diversi strumenti automatizzati (ad es. il badge, normalmente utilizzato presso le pubbliche amministrazioni, se del caso associabile a Pin individuale), risulterebbero inadatti a realizzare legittimi obiettivi di efficienza nell'attività di gestione del personale. Così come non sono stati indicati i motivi in base ai quali non sarebbe possibile effettuare la doverosa attività di controllo sulla corretta esecuzione della prestazione lavorativa dei dipendenti - attraverso gli strumenti posti dall'ordinamento a disposizione dei dirigenti (o comunque del personale direttivo) - stante l'impossibilità, per alcune specifiche figure apicali, di garantire la quotidiana presenza in sede"*, sia con Provvedimento del 17 novembre 2010 "Trasporto: impronte digitali solo in casi particolari", in base al quale affermava che *"Secondo il costante orientamento del Garante, l'utilizzo dei dati biometrici può essere giustificato solo in casi particolari, in relazione alle finalità e al contesto in cui essi sono trattati e, in relazione ai luoghi di lavoro, per presidiare accessi ad "aree sensibili", in considerazione della natura delle attività ivi svolte: si pensi, ad esempio, a processi produttivi pericolosi o sottoposti a segreti di varia natura o al fatto che particolari locali siano destinati alla custodia di beni, documenti segreti o riservati e/o oggetti di valore (in tal senso, vedi il punto 4.1 delle "Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati", emanate dall'Autorità in data 23 novembre 2006*".

(14) Cfr. Provvedimento n. 60 del 16 febbraio 2017, Verifica preliminare. Sistema di controllo accessi biometrico facciale.

a) per gli strumenti che consentono il semplice accesso ed uscita ai locali aziendali senza che il loro uso venga registrato (in particolare dai sistemi informativi aziendali), non necessita alcuna particolare procedura;
b) se, invece, gli strumenti (ad esempio il badge con banda magnetica o microchip) memorizzano soltanto gli orari di entrata ed uscita da parte del sistema informativo aziendale, in base all'art. 4, legge n. 300/1970, per il loro uso legittimo è richiesto al datore di lavoro di fornire al lavoratore adeguata informazione sulle sue modalità d'uso e sulle modalità di effettuazione dei controlli, nel rispetto di quanto disposto dal D.Lgs. n. 196/2003 sulla privacy. Le informazioni così raccolte sono utilizzabili dal datore di lavoro per tutti i fini connessi al rapporto di lavoro, ivi comprese le eventuali sanzioni disciplinari;
c) se, infine, gli strumenti, oltre al controllo degli accessi e delle presenze, consentono di rilevare e memorizzare anche gli spostamenti interni ed esterni all'azienda, la loro liceità è subordinata alla stipulazione di uno specifico accordo sindacale o, nel caso questo non sia stato concluso, ad una autorizzazione dell'Ispettorato del lavoro, territorialmente competente. In tal senso si è espressa la Corte di cassazione, affermando che "*Un'apparecchiatura di controllo predisposta dal datore di lavoro, sia pure a vantaggio dei dipendenti, per la rilevazione non solo dei dati di entrata e uscita dall'azienda, ma anche dell'osservanza dei doveri di diligenza nel rispetto dell'orario di lavoro e della correttezza dell'esecuzione della prestazione lavorativa, costituisce un illegittimo strumento di controllo a distanza, se non autorizzata dall'ispettorato del lavoro o non concordata con le rappresentanze sindacali. La rilevazione dell'orario di entrata e di uscita dall'azienda mediante l'uso del badge da parte dell'azienda si risolve, oltre che in un controllo sull'orario di lavoro, anche in un accertamento sul quantum della prestazione, rientrante nella fattispecie prevista dall'art. 4, comma 2, legge n. 300/1970 (fattispecie relativa a sistema badge in grado di registrare da remoto i dati riguardanti gli orari di ingresso e uscita, le sospensioni, i permessi e le pause, così realizzando un controllo continuo, permanente e globale)*" (15).
La violazione da parte del datore di lavoro degli adempimenti previsti dalla legge a suo carico (informativa ai lavoratori ed eventualmente anche accordo sindacale o autorizzazione dell'Ispettorato del lavoro) determinerà con tutta probabilità l'annullamento degli eventuali provvedimenti adottati dal datore di lavoro nei confronti dei lavoratori che abbiano violato i loro doveri contrattuali. Non così, invece, nel caso in cui i comportamenti dei lavoratori configurino anche un illecito di natura penale. In tal caso, infatti, gli elementi acquisiti mediante l'uso degli strumenti di controllo di cui abbiamo trattato in queste note sono stati ritenuti validi sotto il profilo penale: "*È quindi possibile affermare il seguente principio di diritto: in tema di apparecchiature di controllo dalle quali derivi la possibilità di verificare a distanza l'attività dei lavoratori, le garanzie procedurali previste dall'art. 4, secondo comma, dello Statuto dei lavoratori non trovano applicazione quando si procede all'accertamento di fatti che costituiscono reato. Tali garanzie riguardano solo l'utilizzabilità delle risultanze delle apparecchiature di controllo nei rapporti interni, di diritto privato, fra datore di lavoro e lavoratore; la loro eventuale inosservanza non assume pertanto alcun rilievo nell'attività di repressione di fatti costituenti reato, al cui accertamento corrisponde sempre l'interesse pubblico alla tutela del bene penalmente protetto, anche qualora sia possibile identificare la persona offesa nel datore di lavoro*" (16).

(15) Cass. civ., sez. lav., 14 luglio 2017, n. 17531, in *Guida dir.*, 2017, 33, 68. Conforme Cass. civ., sez. lav., 13 maggio 2016, n. 9904, in *Mass. giust. civ.*, 2016.

(16) Cass. pen., sez. II, 12 maggio 2016 n. 33567, in *Cass. pen.*, 2017, 1, 267. Conforme Cass. pen., sez. VI, 4 giugno 2013 n. 30177, in *Ced Cass. pen.*, 2013.

Approfondimenti

Codice civile

Articolo 2086 - ***Direzione e gerarchia nella impresa*** - [I] L'imprenditore è il capo dell'impresa e da lui dipendono gerarchicamente i suoi collaboratori.
Articolo 2087 - ***Tutela delle condizioni di lavoro*** - [I]. L'imprenditore è tenuto ad adottare nell'esercizio dell'impresa le misure che, secondo la particolarità del lavoro, l'esperienza e la tecnica, sono necessarie a tutelare l'integrità fisica e la personalità morale dei prestatori di lavoro.

Legge 20 maggio 1970, n. 300

Articolo 4 - ***Impianti audiovisivi e altri strumenti di controllo***
1. Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo, gli impianti e gli strumenti di cui al primo periodo possono essere installati previa autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali, della sede centrale dell'Ispettorato nazionale del lavoro. I provvedimenti di cui al terzo periodo sono definitivi.
2. La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.
3. Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili 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.

D.Lgs. n. 196/2003 - Codice in materia di protezione dei dati personali

Articolo 114 - ***Controllo a distanza*** - 1. Resta fermo quanto disposto dall'articolo 4, legge 20 maggio 1970, n. 300:

Articolo 13, commi 4 e 5 - ***Informativa***
4. Se i dati personali non sono raccolti presso l'interessato, l'informativa di cui al comma 1, comprensiva delle categorie di dati trattati, è data al medesimo interessato all'atto della registrazione dei dati o, quando è prevista la loro comunicazione, non oltre la prima comunicazione.
5. La disposizione di cui al comma 4 non si applica quando: a) i dati sono trattati in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria; b) i dati sono trattati ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento; c) l'informativa all'interessato comporta un impiego di mezzi che il Garante, prescrivendo eventuali misure appropriate, dichiari manifestamente sproporzionati rispetto al diritto tutelato, ovvero si riveli, a giudizio del Garante, impossibile.
Articolo 24 - ***Casi nei quali può essere effettuato il trattamento senza consenso***
1. Il consenso non è richiesto, oltre che nei casi previsti nella Parte II, quando il trattamento:
a) è necessario per adempiere ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;
b) è necessario per eseguire obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato;
e) è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se la medesima finalità riguarda l'interessato e quest'ultimo non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere, il consenso è manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato. Si applica la disposizione di cui all'articolo 82, comma 2;
f) con esclusione della diffusione, è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento, nel rispetto della vigente normativa in materia di segreto aziendale e industriale;
g) con esclusione della diffusione, è necessario, nei casi individuati dal Garante sulla base dei principi sanciti dalla legge, per perseguire un legittimo interesse del titolare o di un terzo destinatario dei dati, qualora non prevalgano i diritti e le libertà fondamentali, la dignità o un legittimo interesse dell'interessato.