CONFINDUSTRIA

CIRCOLARE

"IL NUOVO ART. 4 DELLO STATUTO DEL LAVORATORI: PROFILI PRIVACY"

Premessa di raccordo con la nuova disciplina lavoristica

L'art. 23 del d.lgs n. 151/2015 riscrive la disciplina sui controlli a distanza dei lavoratori, contenuta nell'art. 4 dello Statuto dei lavoratori (legge n. 300/1970, di seguito anche "Statuto"), al fine di adeguarla alle nuove modalità di svolgimento dell'attività lavorativa.

In particolare, la norma:

- elimina il generale divieto di controllo a distanza dei lavoratori;
- mantiene, semplificandone la procedura concertativa-autorizzativa, la possibilità di installare, per esigenze organizzative e produttive, nonché per la sicurezza del lavoro, apparecchiature dalle quali derivi anche la possibilità del controllo a distanza dei lavoratori (*cd*. controlli preterintenzionali). Al riguardo, la nuova norma introduce anche le finalità di tutela del patrimonio aziendale, che legittimano i *cd*. controlli difensivi, già ammessi - con qualche limite - dalla giurisprudenza (co. 1). Tuttavia, la necessità che ricorrano finalità predeterminate dalla legge porta a escludere l'utilizzo di strumenti tecnologici il cui unico scopo sia quello di consentire un controllo a distanza dell'attività dei lavoratori;
- esclude dalla procedura concertativo-autorizzativa, nonché dalle finalità predeterminate, l'utilizzo degli strumenti necessari a eseguire la prestazione lavorativa (*cd*. strumenti di lavoro) e l'installazione di strumenti per la registrazione degli accessi e delle presenze. Come osservato anche dal Garante privacy, la possibilità di controllare l'adempimento della prestazione attraverso l'uso di strumenti di lavoro diviene un "effetto naturale del contratto", discendendo dalla stessa costituzione del rapporto di lavoro: l'unico requisito finalistico applicabile a tale controllo è quello connesso al rapporto di lavoro (co. 2);
- consente di utilizzare i dati raccolti mediante i controlli preterintenzionali e quelli sugli strumenti di lavoro e di rilevazione delle presenze ***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 Codice privacy** (co. 3). Come anticipato, mentre con riferimento agli strumenti di lavoro e di rilevazione delle presenze, il controllo sull'adempimento degli obblighi derivanti dal contratto discende dalla stessa costituzione del rapporto di lavoro, con riferimento agli altri strumenti tecnologici, tale controllo è da ritenersi "incidentale", poiché non direttamente connesso alle finalità – predeterminate – di utilizzo degli stessi.

1) Il rispetto della normativa privacy

1.a) I principi generali

Come anticipato, la possibilità di utilizzare *a tutti i fini connessi al rapporto di lavoro* i dati forniti dagli strumenti tecnologici (di lavoro e non) è subordinata a:

- l'informazione del lavoratore circa le *modalità d'uso degli strumenti e di effettuazione dei controlli*;
- il rispetto del Codice privacy (d.lgs n. 196/2003, di seguito anche "Codice").

Quanto all'informativa sulle modalità di utilizzo degli strumenti tecnologici e di esecuzione dei controlli, appare ragionevole ritenere che costituisca un adempimento distinto ma integrabile con la *cd*. informativa privacy (art. 13 del Codice privacy). Infatti, mentre la prima è finalizzata a informare il lavoratore sulle modalità d'uso degli strumenti tecnologici e sugli eventuali controlli, la seconda è finalizzata a informare il lavoratore sui trattamenti dei dati connessi all'utilizzo degli strumenti (es. finalità e caratteristiche del trattamento, diritti degli interessati). Tale impostazione sembrerebbe confermata anche dal Garante privacy che, nelle Linee Guida per l'utilizzo della posta elettronica e internet, ha distinto le finalità di trasparenza sul corretto utilizzo degli strumenti messi a disposizione del lavoratore e sui controlli, da quelle di trasparenza in merito ai trattamenti conseguenti. Considerato lo stretto legame tra l'informativa *ex* art. 4, co. 3 dello Statuto e l'informativa *ex* art. 13 del Codice privacy, si ritiene che anche la prima vada resa singolarmente a ciascun lavoratore, al fine di indicargli specificamente le modalità di utilizzo degli strumenti allo stesso assegnati e dello svolgimento dei controlli, nonché la possibilità di utilizzare le informazioni acquisite a tutti i fini connessi al rapporto di lavoro ai sensi del nuovo art. 4, co. 3 dello Statuto. Tale circostanza non sembrerebbe escludere la redazione di disciplinari interni, validi per gruppi di lavoratori che svolgono le stesse mansioni ovvero per gruppi di lavoratori che, pur svolgendo mansioni differenti, utilizzano i medesimi strumenti (v. Linee Guida per l'utilizzo della posta elettronica e internet, par. 3.2). In ogni caso, sarebbe opportuno che la diffusione di tali disciplinari tra i lavoratori interessati avvenisse con modalità tali da assicurarne la comunicazione personale (es. consegna del disciplinare, invio del disciplinare per *e-mail*).

Quanto al rispetto del Codice privacy, esso costituisce un ulteriore requisito di legittimità dell'esercizio dei poteri di controllo e disciplinare da parte del datore di lavoro.

In particolare, **la normativa privacy deve improntare tutte le operazioni di trattamento connesse all'utilizzo degli strumenti tecnologici**: dalla mera raccolta dei dati, alla loro registrazione, conservazione, consultazione, estrazione, raffronto, utilizzo, comunicazione, distruzione, ecc. In altri termini, la normativa privacy è idonea a condizionare l'ampiezza e la tipologia del controllo, al fine di tutelare il diritto alla riservatezza del lavoratore.

Tuttavia, come osservato dal Gruppo di lavoro sulla protezione dei dati (*cd*. GdL *ex* art. 29), *la privacy non è un diritto assoluto* (Parere n. 8/2001 sul trattamento di dati personali nell'ambito dei rapporti di lavoro). È necessario, infatti, ricercare un giusto equilibrio fra la tutela della riservatezza e la tutela degli altri interessi connessi all'esistenza di un rapporto di lavoro.

Come affermato dal GdL *ex* art. 29, i lavoratori, fino a quando operano all'interno di una determinata organizzazione, *devono accettare un certo grado di invasione della loro privacy e devono fornire al datore di lavoro determinate informazioni personali. Il datore di lavoro ha un interesse legittimo a trattare dati personali dei propri dipendenti per scopi leciti e legittimi che siano necessari per il normale sviluppo del rapporto di lavoro e per lo svolgimento delle attività di impresa*.

Il punto non è, pertanto, se il trattamento di dati sul luogo di lavoro sia di per sé un'attività lecita o meno. Il punto fondamentale sono i limiti che la legislazione sulla protezione dei dati impone rispetto a tali attività, ovvero, rovesciando i termini, le motivazioni che possono giustificare la raccolta ed il trattamento ulteriore di dati personali relativi ad un lavoratore. …. Il livello tollerato di invasione della privacy dipenderà in misura consistente dalla natura dell'attività lavorativa e dalle circostanze specifiche che si accompagnano e interagiscono con il rapporto di lavoro e possono influirvi.

Quanto alle regole che devono ispirare i trattamenti dei dati derivanti dall'utilizzo di strumenti tecnologi nell'ambito lavorativo, rilevano in primo luogo i principi generali dettati dal Codice privacy. Il riferimento è a:

- i **principi di semplificazione, armonizzazione ed efficacia**, che riguardano non solo le modalità di esercizio dei diritti degli interessati, ma anche gli adempimenti del titolare (art. 2). Tali principi sono volti a garantire la predisposizione di *policy* privacy aziendali utili e semplici, che consentano la tutela della riservatezza del lavoratore, senza irrigidire con pratiche burocratiche le attività del titolare-datore di lavoro;

- il **principio di liceità** (art. 11, co. 1, lett. a), che impone il rispetto della normativa – non solo privacy – che interessa la fattispecie. Ad esempio, con riferimento all'art. 4 dello Statuto, il trattamento derivante dall'utilizzo di strumenti *ex* comma 1 è da ritenersi lecito se il datore di lavoro ha rispettato la procedura concertativo-autorizzativa;
- il **principio di necessità** (art. 11, co. 1, lett. a), inteso come presidio della necessità del trattamento (solo quando necessario) e affermazione dell'essenzialità dei dati personali utilizzati (*cd*. minimizzazione). Sul piano operativo, il principio comporta che i sistemi informativi e i programmi informatici debbano essere impostati dal datore di lavoro, riducendo al minimo l'utilizzazione dei dati personali e dei dati identificativi del lavoratore in relazione alle finalità perseguite;
- il **principio di correttezza**, che deve informare il trattamento in ogni suo profilo (art. 11, co. 1, lett. a). In particolare, il principio impone di ispirare il trattamento a un canone di trasparenza, rendendo note ai lavoratori le caratteristiche essenziali dei trattamenti svolti mediante il monitoraggio degli strumenti tecnologici. Come osservato dal GdL *ex* art. 29, *un datore di lavoro può avere un interesse legittimo a verificare il rendimento dei propri dipendenti attraverso la valutazione dei risultati ottenuti (ad esempio, quanti casi siano stati trattati, quante chiamate telefoniche abbiano avuto risposta, ecc.)* (…) *Se un'attività di sorveglianza del genere dovesse svolgersi senza fornire al personale le opportune informazioni, il trattamento dei dati relativi ai dipendenti sarebbe in contrasto con le disposizioni della direttiva 95/46/CE*. In ambito contrattuale, il principio di correttezza trova una rispondenza sistematica nel principio di buona fede sancito dal codice civile, pertanto, lo stesso è idoneo a incidere anche sul comportamento degli interessati (es. si pensi alla manifestazione del consenso o all'esercizio dei diritti *ex* art. 7 del Codice). Con specifico riguardo al rapporto di lavoro, il Garante privacy ha sottolineato che, in caso di trattamenti *svolti nel rispetto dei principi della legge*, la necessità di garantire la semplificazione degli adempimenti e la correttezza nelle relazioni negoziali impone, sia al datore di lavoro che al lavoratore, di evitare strumentalizzazioni delle norme sulla privacy *allo scopo di danneggiare o rendere più onerosa e difficile l'attività della controparte* (Parere 28 ottobre 1999);
- i **principi di determinatezza, legittimità ed esplicitazione del fine** perseguito dal trattamento (art. 11, co. 1, lett. b). In base a tali principi, il trattamento deve supporre una finalità legittima, specifica e manifesta all'atto della raccolta e i successivi utilizzi devono essere compatibili con lo scopo dichiarato. Con riferimento ai trattamenti dei dati derivanti dall'utilizzo in ambito lavorativo di dispositivi tecnologici, la riforma dell'art. 4 dello Statuto ha confermato le finalità connesse a esigenze organizzative, produttive, di sicurezza sul lavoro e di tutela del patrimonio aziendale e ha legittimato quelle connesse al rapporto di lavoro, comprese quelle di tipo disciplinare. Tuttavia, le finalità di tipo disciplinare potranno soddisfare il requisito di legittimità ai fini privacy solo se il controllo operato *ex ante* sul lavoratore non pregiudichi in modo ingiustificato i suoi diritti e libertà. A tal fine, rilevano i **principi di pertinenza e non eccedenza dei dati trattati** (art. 11, co. 1, lett. d), che riguardano il rapporto tra finalità e dati e, quindi, la proporzionalità di questi ultimi rispetto agli scopi identificati e alle reali esigenze dell'organizzazione. Come osservato dal GdL ex art. 29, in ambito lavoristico i principi di pertinenza e non eccedenza presentano numerose sfaccettature. Tuttavia, il loro *effetto primario è la necessità per il datore di lavoro di trattare i dati personali nella maniera meno invasiva possibile. A tale riguardo, si dovrebbero tenere in considerazione vari elementi: i rischi connessi, la quantità di dati oggetto del trattamento, le finalità di quest'ultimo, ecc.*;
- il **principio della conservazione dei dati** per il tempo necessario a realizzare gli scopi del trattamento (art. 11, co. 1, lett. e);
- la **necessaria legittimazione soggettiva** al trattamento, che impone di limitare ai soli soggetti preposti l'autorizzazione allo svolgimento di attività di monitoraggio sul lavoro;
- l'**informativa preventiva** (art. 13).

Sulla base di tali considerazioni, ogni attività di monitoraggio in ambito lavoristico deve costituire una risposta proporzionata del datore di lavoro ai rischi che si trova ad affrontare, tenendo conto del legittimo interesse dei lavoratori alla privacy. I dati personali detenuti o utilizzati nel corso delle attività di

monitoraggio devono essere adeguati, pertinenti e non eccedenti rispetto alle finalità che giustificano il controllo, che in ogni caso deve essere condotto nella maniera meno invasiva possibile.

1.b) I Provvedimenti del Garante privacy

Il rispetto della normativa privacy, quale presupposto per l'esercizio dei poteri di controllo e disciplinari da parte del datore di lavoro, riguarda non solo le singole disposizioni contenute nel Codice, ma anche i provvedimenti adottati dal Garante privacy.

L'art. 154 del Codice, infatti, nel disciplinare i compiti dell'Autorità, attribuisce alla stessa il potere di disporre anche d'ufficio misure necessarie - od opportune - a rendere il trattamento conforme alla disciplina privacy (*cd*. poteri prescrittivi/inibitori).

Sulla base di tali poteri e durante la vigenza del precedente art. 4 dello Statuto, il Garante privacy ha adottato diversi provvedimenti aventi a oggetto trattamenti di dati connessi al rapporto di lavoro e idonei a incidere sullo svolgimento dei controlli.

Il riferimento è, in particolare, a:

1. il Provvedimento 1 marzo 2007, recante le Linee Guida per l'utilizzo della posta elettronica e internet;
2. il Provvedimento 8 aprile 2010, in materia di trattamento di dati personali effettuato tramite sistemi di videosorveglianza;
3. il Provvedimento 4 ottobre 2011 sui sistemi di localizzazione dei veicoli nell'ambito del rapporto di lavoro;
4. il Provvedimento 12 novembre 2014 in tema di biometria.

Tali provvedimenti declinano in termini operativi i principi generali dettati dal Codice privacy, prescrivendo alle imprese-titolari del trattamento specifici adempimenti e limiti alla raccolta e all'utilizzo dei dati riguardanti i lavoratori.

In considerazione delle modifiche che hanno riguardato l'art. 4 dello Statuto e in assenza di un intervento specifico da parte dell'Autorità, occorre verificare se le prescrizioni contenute nei predetti provvedimenti siano da considerarsi ancora efficaci e in che termini possano impattare sullo svolgimento dei controlli e sull'esercizio dei conseguenti poteri disciplinari.

In via preliminare, occorre osservare che la maggior parte dei predetti provvedimenti muove dal presupposto delle garanzie previste dalla precedente formulazione dell'art. 4 dello Statuto (accordo sindacale o autorizzazione amministrativa), al fine di: *i)* stabilire la liceità del trattamento; *ii)* applicare la disciplina del *cd*. bilanciamento di interessi, esonerando il titolare dall'acquisizione del consenso al trattamento dei dati.

Sul punto, si ritiene che la nuova normativa non impatti sui predetti provvedimenti relativamente agli strumenti impiegati per le finalità indicate nel comma 1: per l'utilizzo di tali strumenti, l'art. 4 dello Statuto continua a richiedere l'accordo sindacale o, in difetto, l'autorizzazione amministrativa, pertanto, tali adempimenti continueranno a rilevare in termini di liceità e bilanciamento di interessi.

Quanto, invece, agli effetti sui provvedimenti relativi agli strumenti tecnologici di lavoro, appare ragionevole ritenere che l'accordo sindacale ovvero l'autorizzazione amministrativa non costituiscano più condizioni di liceità e che i relativi trattamenti siano da ricondurre tra quelli necessari all'esecuzione di un contratto di cui è parte l'interessato (vale a dire il lavoratore) e, di conseguenza, realizzabile senza il consenso di quest'ultimo.

Di seguito, una breve disamina dei Provvedimenti e dei relativi effetti sull'operatività dell'art. 4 dello Statuto dei lavoratori.

1.b.1) Le Linee Guida per l'utilizzo della posta elettronica e internet

Le Linee Guida prescrivono al datore di lavoro alcune misure per conformare alla normativa privacy **il trattamento dei dati personali effettuato per verificare il corretto utilizzo nel rapporto di lavoro della posta elettronica e della rete internet**. Le Linee Guida, quindi, si inseriscono tra le previsioni privacy volte a legittimare e definire il controllo sugli strumenti di lavoro *ex* comma 2 dell'art. 4 dello Statuto.

Sul tema, il Garante privacy ha ribadito la prerogativa del datore di lavoro di controllare l'effettivo adempimento della prestazione lavorativa e, se necessario, il corretto utilizzo degli strumenti di lavoro (par. 4). Tali controlli determinano un trattamento di dati personali riferiti o riferibili ai lavoratori, che deve svolgersi in conformità al Codice privacy.

In osservanza del principio di:

- **correttezza**, il Garante privacy ha prescritto al datore di lavoro l'onere di specificare le modalità di utilizzo della posta elettronica e della rete internet da parte dei lavoratori, indicando chiaramente le modalità di uso degli strumenti messi a disposizione e se, in che misura e con quali modalità vengano effettuati controlli. A tal fine, l'Autorità suggerisce l'adozione di un disciplinare interno, da pubblicizzare adeguatamente tra i lavoratori interessati (par. 3.2). Sulla permanenza dell'adempimento non sorgono dubbi, considerato che il nuovo art. 4 dello Statuto subordina a tale informativa la possibilità di utilizzare a tutti i fini - connessi il rapporto di lavoro - i dati forniti dagli strumenti di lavoro. Ne consegue che, in merito ai monitoraggi sull'utilizzo della posta elettronica e della rete internet, rimangono invariati gli oneri informativi relativi alle modalità di impiego degli strumenti e agli eventuali controlli e conseguenze attivabili. Accanto all'onere del datore di lavoro di prefigurare e pubblicizzare una *policy* interna rispetto al corretto uso dei mezzi e agli eventuali controlli, le Linee Guida ribadiscono il dovere di informare comunque gli interessati ai sensi dell'art. 13 del Codice privacy (par. 3.3). Anche tale adempimento deve considerarsi ancora attuale, essendo l'informativa privacy la prima condizione di liceità di tutte le operazioni di trattamento, comprese quelle eseguite in virtù dei controlli. Sul piano operativo, ai fini dell'adeguamento alla nuova disciplina, sarebbe opportuno verificare l'attualità dei disciplinari in atto e informare in ogni caso i lavoratori che, ai sensi del nuovo art. 4, co. 3 dello Statuto, le informazioni acquisite possono essere utilizzate a tutti i fini connessi al rapporto di lavoro;
- **necessità**, l'Autorità ribadisce l'opportunità di adottare un approccio di tipo preventivo e non repressivo, sottolineando l'onere del datore di lavoro di implementare tutte le misure tecnologiche volte a minimizzare l'uso dei dati identificativi e scongiurare controlli successivi sul lavoratore;
- **pertinenza e non eccedenza**, il Garante privacy propone di impostare lo svolgimento dei controlli in termini di gradualità, al fine di evitare interferenze ingiustificate sui diritti dei lavoratori e dei soggetti esterni che ricevono o inviano *e-mail* private. Ad avviso dell'Autorità, in presenza di un evento dannoso o di una situazione di pericolo non impediti da preventivi accorgimenti tecnici, il datore di lavoro deve privilegiare un controllo preliminare su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree. Il controllo anonimo può concludersi con un avviso generalizzato relativo a un rilevato utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. L'avviso può essere circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia. In assenza di successive anomalie, non è di regola giustificato effettuare controlli su base individuale. Sul punto si ritiene che, nonostante l'unico requisito finalistico applicabile al controllo sugli strumenti di lavoro sia quello connesso al rapporto di lavoro, i principi di necessità, pertinenza e non eccedenza debbano continuare a improntare i trattamenti connessi alle attività di controllo, affinché queste non risultino "prolungate, costanti o indiscriminate";
- **conservazione**, l'Autorità ha ribadito la necessità di programmare i sistemi *software* in modo da cancellare periodicamente e automaticamente (attraverso procedure di sovraregistrazione) i dati personali relativi agli accessi a internet e al traffico telematico, la cui conservazione non sia necessaria. In assenza di particolari esigenze tecniche o di sicurezza, la conservazione dei dati relativi all'uso degli strumenti elettronici deve essere giustificata da una finalità specifica e comprovata e limitata al tempo necessario — e predeterminato — a raggiungerla. In questi casi, il trattamento dei dati personali deve

essere limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate.

Infine, la stessa Autorità ha vietato ai datori di lavoro di effettuare trattamenti di dati personali mediante sistemi *hardware* e *software* che mirano al controllo a distanza di lavoratori, svolti in particolare mediante: *i)* la lettura e la registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio *e-mail*; *ii)* la riproduzione e l'eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore; *iii)* la lettura e la registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo; *iv)* l'analisi occulta di PC portatili affidati in uso.

1.b.2) La videosorveglianza

Con il Provvedimento 8 aprile 2010, il Garante privacy ha prescritto misure per i trattamenti dei dati derivanti dall'installazione di sistemi di videosorveglianza.

Rispetto all'utilizzo di tali strumenti nei luoghi di lavoro, il lavoratore continua a godere di una duplice tutela: *i)* quella prevista Codice privacy, che coincide con quella di qualsiasi altro soggetto la cui immagine venga rilevata dal sistema; *ii)* quella prevista dall'art. 4, co. 1 dello Statuto che, in ogni caso, non consente l'utilizzo di impianti audiovisivi per finalità di controllo a distanza del lavoratore e ne subordina l'installazione all'esistenza di specifiche finalità e allo svolgimento di una procedura concertativa-autorizzativa.

Tuttavia, rispetto alla disciplina previgente, il nuovo art. 4, co. 3 dello Statuto consente l'utilizzo a tutti i fini del rapporto di lavoro anche delle informazioni acquisite dall'impianto di videosorveglianza, purché lo stesso sia stato installato per finalità specifiche, il lavoratore sia stato informato dell'impiego di tale strumento e dello svolgimento di eventuali controlli e previo rispetto della normativa privacy.

Il provvedimento sulla videosorveglianza, quindi, assume rilevanza ai fini di tale "nuovo" utilizzo, determinandone limiti e condizioni.

Quanto alle misure prescritte dal Garante privacy, oltre agli obblighi di informativa, di istanza di verifica preliminare e di notificazione, che rilevano principalmente ai fini privacy, si segnalano quelle relative a:

- le riprese, che non devono riguardare luoghi, persone o particolari non rilevanti;
- la durata della conservazione delle immagini, che non può essere superiore alle 24 ore successive alla rilevazione, fatte salve specifiche esigenze che rendono necessaria una conservazione prolungata (festività o chiusura di uffici ed esercizi, richieste investigative dell'autorità giudiziaria o della polizia)

che incidono maggiormente anche sui limiti – in termini di modalità e termini - dell'utilizzo delle immagini ai sensi del comma 3.

Quanto, poi, all'informazione in merito all'utilizzo dell'impianto e all'eventualità che vengano effettuati controlli sulle immagini rilevate, si ritiene che essa debba riguardare:

- la presenza dell'impianto audiovisivo, le finalità predeterminate *ex* comma 1, il funzionamento, i tempi di conservazione delle immagini, l'accesso alle immagini riservato a soggetti specificamente abilitati, la possibilità che le immagini siano fornite all'autorità giudiziaria o alla polizia giudiziaria in relazione a un'attività investigativa in corso, la possibilità che le immagini vengano visionate in occasione di istanze di accesso da parte di interessati ai sensi dell'art. 7 del Codice;
- gli accessi che possono determinare un controllo "incidentale", la tipologia e la modalità di controllo, la circostanza che le immagini visionate possano essere utilizzate a fini disciplinari qualora si ravvisi una violazione degli obblighi derivanti dal contratto di lavoro.

1.b.3) I sistemi di localizzazione dei veicoli aziendali

Con il Provvedimento 4 ottobre 2011 il Garante privacy ha indicato una serie di misure per il trattamento dei dati connesso all'utilizzo di sistemi di localizzazione dei veicoli aziendali per esigenze organizzative o produttive ovvero per la sicurezza sul lavoro (es. per soddisfare esigenze logistiche e impartire istruzioni tempestive al conducente del veicolo; per elaborare rapporti di guida ai fini della retribuzione del conducente; per commisurare i costi da imputare alla clientela; per un'efficiente gestione e manutenzione del parco auto). Le informazioni relative all'ubicazione dei veicoli, infatti, sono da considerarsi dati personali in quanto direttamente o indirettamente associabili al lavoratore assegnatario del mezzo. Pertanto, il relativo trattamento deve avvenire in conformità alla normativa privacy.

Con riferimento ai trattamenti derivanti dall'utilizzo di sistemi di localizzazione in ambito lavoristico, il Garante privacy ha prescritto ai titolari-datori di lavoro le seguenti misure:

- in osservanza del **principio di necessità**, la posizione del veicolo non deve essere monitorata continuamente, ma solo quando ciò sia necessario per il perseguimento delle finalità perseguite;
- in osservanza dei **principi di pertinenza e non eccedenza**, possono formare oggetto di trattamento solo i dati pertinenti, come quelli relativi alla posizione del veicolo, alla distanza percorsa, ai tempi di percorrenza, al carburante consumato, alla velocità media del veicolo. Inoltre, i tempi di conservazione dei dati devono essere commisurati alle specifiche finalità perseguite;
- in osservanza del **principio di correttezza**, gli interessati devono essere adeguatamente informati sulle caratteristiche del sistema e sulla natura dei dati trattati, nonché sugli altri elementi indicati dall'art. 13 del Codice privacy. A tal fine, sul veicolo devono essere collocate delle vetrofanie o avvisi che segnalino la geolocalizzazione del veicolo;
- in osservanza del **principio di liceità e della disciplina del bilanciamento di interessi**, l'adozione delle garanzie lavoristiche legittima i datori di lavoro a trattare i dati di localizzazione in assenza del consenso del lavoratore.

Resta fermo, in ogni caso, l'obbligo di notificazione all'Autorità del trattamento dei dati di localizzazione.

Il provvedimento assume rilevanza ai fini dell'utilizzo dei dati di localizzazione *ex* art. 4, co. 3 dello Statuto. In particolare, lo stesso rileva ai fini del rispetto della normativa privacy, nonché quale limite – in termini di tipologia di informazioni e tempi di conservazione delle stesse - ai fini di un controllo "finalizzato" o "incidentale" sull'adempimento degli obblighi derivanti dal contratto di lavoro (a seconda che il sistema rientri tra gli strumenti *ex* comma 2 o tra quelli *ex* comma 1).

In ogni caso, si segnala che il lavoratore deve essere informato delle caratteristiche del sistema di localizzazione, delle finalità e delle modalità d'uso, nonché delle situazioni che possono determinare un controllo "incidentale", la tipologia e la modalità del controllo e la circostanza che le immagini visionate possano essere utilizzate a fini disciplinari qualora si ravvisi una violazione degli obblighi derivanti dal contratto di lavoro.

1.b.4) Il trattamento dei dati biometrici

Con il Provvedimento 12 novembre 2014 il Garante privacy ha adottato le Linee Guida sul trattamento dei dati biometrici (es. l'immagine dell'impronta digitale, l'immagine dell'iride o della retina, la registrazione della voce, la topografia della mano, la firma grafometrica).

I dati biometrici riguardano le caratteristiche biologiche (es. le impronte digitali, la struttura venosa della mano o delle dita, la struttura vascolare della retina, la forma dell'iride) o comportamentali (es. la dinamica dell'apposizione della firma, il tipo di andatura, l'emissione della voce) di una persona e ne consentono l'identificazione univoca. Si tratta, quindi, di informazioni delicate che denotano una stretta relazione tra il corpo e l'identità di un soggetto e che, pertanto, necessitano di una tutela privacy rafforzata.

Con riferimento al trattamento dei dati biometrici dei lavoratori, dalle Linee Guida e dai provvedimenti specifici adottati dall'Autorità, si ricava che:

- i dati biometrici possono essere utilizzati soltanto in casi particolari, tenuto conto delle finalità perseguite dal titolare e del contesto in cui il trattamento viene effettuato e che, quindi, non può ritenersi lecito l'impiego generalizzato e indiscriminato di dati biometrici, specie se funzionale a soddisfare sommarie esigenze di sicurezza, ovvero a perseguire finalità di natura essenzialmente amministrativa (*Provv*. 23 gennaio 2008; *Provv*. 10 marzo 2011; *Provv*. 16 febbraio 2012; *Provv*. 29 marzo 2012, n. 127);
- l'installazione di sistemi di rilevazione di dati biometrici è ammessa esclusivamente per presidiare accessi ad "aree sensibili", in considerazione della natura delle attività svolte (es. processi produttivi pericolosi o sottoposti a segreti di varia natura) o dei beni custoditi (es. locali destinati alla custodia di documenti segreti o riservati ovvero di oggetti di valore) oppure per consentire l'utilizzo di apparati e macchinari pericolosi ai soli soggetti qualificati; l'impronta digitale o l'emissione vocale possono essere utilizzate per l'autenticazione informatica (accesso a banche dati o a PC aziendali); la firma grafometrica per la sottoscrizione di documenti informatici;
- l'installazione di sistemi di rilevazione di dati biometrici non è consentita per finalità di rilevazione delle presenze sul luogo di lavoro (*Provv*. 21 luglio 2005; *Provv*. 2 ottobre 2008; *Provv*. 15 ottobre 2009; *Provv*. 29 ottobre 2009; *Provv*. 20 ottobre 2011; *Provv*. 31 gennaio 2013; *Provv*. 30 maggio 2013; *Provv*. 1° agosto 2013).

Nei casi in cui è consentito, il trattamento dei dati biometrici deve avvenire nel rispetto di:

- il **principio di necessità**. I sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi. Prima di procedere all'utilizzo di un sistema biometrico, pertanto, occorre valutare se le stesse finalità possano essere perseguite mediante dati anonimi oppure tramite il sistema biometrico ma con modalità tali da permettere l'individuazione dell'interessato solo in caso di necessità;
- i **principi di liceità, finalità e proporzionalità del trattamento**;
- l'adozione delle **misure di sicurezza**;
- la richiesta di **verifica preliminare** al Garante privacy. L'Autorità ha individuato alcune tipologie di trattamenti in relazione alle quali non è necessaria la presentazione della richiesta di verifica preliminare. Il riferimento è a: *i)* l'autenticazione informatica; *ii)* il controllo di accesso fisico ad aree "sensibili" dei soggetti addetti e utilizzo di apparati e macchinari pericolosi; *iii)* l'so delle impronte digitali o della topografia della mano a scopi facilitativi; *iv)* la sottoscrizione di documenti informatici;
- la **notificazione** del trattamento al Garante privacy;
- l'**informativa** specifica;
- **consenso** dell'interessato, ferme restando le ipotesi di esonero.

Ai fini dell'applicazione dell'art. 4 dello Statuto, l'utilizzo dei sistemi biometrici può rilevare sia ai fini del comma 1, sia ai fini del comma 2.

Occorre, infatti, distinguere i sistemi biometrici funzionali a rendere la prestazione lavorativa o a consentire l'accesso in particolari aree dell'azienda, soggetti alla disciplina di cui al comma 2, da quelli solo accessori della strumentazione soggetti, invece, al comma 1.

In entrambi casi, il datore di lavoro sarà comunque tenuto al rispetto delle garanzie privacy, nonché a informare preventivamente il lavoratore in merito alle caratteristiche del dispositivo e alle relative modalità di utilizzo, nonché allo svolgimento dei controlli e alla possibilità di utilizzare le informazioni acquisite a fini disciplinari qualora si ravvisi una violazione degli obblighi derivanti dal contratto di lavoro.