privacy e diritto del lavoro

La tutela della privacy del lavoratore

Commento a cura dell'avv. Ciro Cafiero, Studio legale Cafiero Pezzali & Associati

Premessa

Il nostro diritto del lavoro ha mutato radicalmente pelle. Da più di qualche anno, lo Statuto dei lavoratori, legge n. 300 del 1970, mostra cedimenti in conseguenza dell'innovazione tecnologica, che ne ha sovvertito le logiche anche sotto il profilo del trattamento dei dati del lavoratore.

Infatti, la tecnologia ha reso accessibili al datore di lavoro dati del lavoratore un tempo protetti da una cortina invalicabile. In tale prospettiva, vuole di seguito farsi luce, con la necessaria sintesi, sui limiti di tale controllo a tutela della privacy del lavoratore ma anche interrogarsi sulla tenuta di tali limiti con particolare riferimento agli sviluppi futuri dello smart working, per rassegnare infine le dovute conclusioni

La tutela della privacy del lavoratore

Gli articoli 4 e 8 dello Statuto dei lavoratori, legge n. 300 del 1970, hanno la finalità di tutelare dai controlli c.d. odiosi il lavoratore (**nota1**) nell'ottica di garantirne la sfera di riservatezza nel segno degli articoli 1, 2, 6, 13, 14 e 15 della Costituzione.

L'articolo 4, invero, limita il potere di c.d. controllo a distanza, ovvero da remoto, dell'attività dei lavoratori mentre l'articolo 8 vieta al datore di lavoro l'indagine sulle opinioni (politiche, sindacali, religiose etc.) del lavoratore.

Tali disposizioni sono il frutto del bilanciamento tra l'esigenza di tutela del lavoratore dai controlli pervasivi del datore di lavoro e l'esigenza di quest'ultimo di sorvegliare il patrimonio aziendale nonché di controllare la prestazione del primo in funzione sia dell'esercizio del potere disciplinare che di quello organizzativo e direttivo (nel segno degli articoli 2086 e 2094 del codice civile).

L'articolo 4, in particolare, ha perseguito la sua finalità di tutela attraverso la previsione di una procedura autorizzatoria ai fini del controllo a distanza del lavoratore, che deve aver luogo o in sede sindacale o presso l'Ispettorato del lavoro.

Ad opera delle modifiche apportate dall'articolo 23 del d.lgs. n. 151 del 2015 (c.d. Jobs Act) (**nota2**) , tale procedura resta obbligatoria con esclusivo riferimento agli strumenti diretti null'altro che al controllo del lavoratore come ad esempio i sistemi di video sorveglianza, e non anche agli strumenti di lavoro, da cui possa derivare il controllo di quest'ultimo, come ad esempio il *table*t, i dispositivi *mobile*, il *pc*.

Ciò in quanto il legislatore ha preso atto che il controllo del lavoratore, che fa uso di tali strumenti, è così immanente alla prestazione di lavoro che viene meno l'utilità di una qualsiasi procedura per autorizzarlo.

Ciò posto, gli articoli 4 e 8 dello Statuto dei lavoratori devono leggersi in combinato disposto con la disciplina sulla privacy, e dunque con il d.lgs. n. 196 del 2003, c.d. Codice della *Privacy*, modificato dal Regolamento (Ue) 679 del 2016 per effetto del d.lgs. 10 agosto 2018, n. 101, in vigore dal 19 settembre 2018.

Secondo tale combinato disposto, la tutela della privacy del lavoratore, nel segno del principio di c.d *accountability*, espresso dal Regolamento europeo, passa per l'osservanza dei due principi fondamentali di *privacy by design* e di *privacy by default*.

Tali principi, in buona sostanza, impongono al titolare dei dati del lavoratore, e dunque al datore di lavoro, di trattare tali dati minimizzando i rischi di un loro trattamento illecito.

Con trattamento illecito, si intende un trattamento in violazione del principio di necessità, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo

l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite (ex art. 3 del Codice della *Privacy*, par. 5.2).
Un trattamento in violazione del principio di correttezza, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori (ex art. 11 del Codice della *Privacy*).
Un trattamento, infine, del principio di non pertinenza e non eccedenza (ex art. 11 del Codice della Privacy) secondo cui: i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime; il datore di lavoro deve trattare i dati "*nella misura meno invasiva possibile*"; le attività di monitoraggio devono essere svolte solo da soggetti preposti ed essere *"mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati*" (a tale riguardo, si veda altresì il Parere n. 8/2001 del Garante per la protezione dai dati personali). (nota3)
A tali principi rimanda anche l'articolo 4 dello Statuto dei lavoratori, come modificato dall'articolo dal d.lgs. n. 151 del 2015, che subordina l'utilizzabilità dei dati del lavoratore al rispetto "*di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196"*.

I nuovi confini della privacy nell'era dello smart working

Se tutto questo è vero, è anche vero che lo *smart working*, introdotto nel nostro ordinamento prima dalla contrattazione collettiva e poi dalla legge n. 81 del 2017, rischia - in un futuro molto prossimo - di indebolire la tenuta delle descritte misure, nazionali ed europee, a tutela della privacy del lavoratore.
In via preliminare, deve osservarsi che il controllo della gran parte dei dati personali e identificativi dello *smart worker* da parte del datore di lavoro è – sin da ora - più che immanente allo svolgimento della prestazione lavorativa dello stesso posto che essa si svolge da remoto e quindi per mezzo di un'ininterrotta connessione di tali dati tra datore di lavoro e lavoratore.
In altri termini, il datore di lavoro entra "comodamente" nei luoghi riconducibili alla sfera privata dello smart worker e che quest'ultimo ha eletto a luogo di svolgimento della prestazione di lavoro.
Ciò posto, alcune tecnologie saranno presto in grado di registrare la fatica o l'emotività del lavoratore ai fini del controllo della sua produttività, e dunque dati appartenenti alla sfera inconscia del lavoratore, con ogni conseguente riflesso, peraltro, in termini di utilizzo di tali informazioni sotto il profilo disciplinare.
In tal senso, si considerino i dispositivi applicabili all'iride per rilevare il grado di attenzione del lavoratore o ancora i rilevatori di stanchezza applicabili alla tastiera del pc connesso alla sede datoriale o, infine, i caschi in grado di legge le interazioni celebrali del lavoratore già sperimentati in Cina.
Si tratta di evenienze che gli articoli 4 e 8 dello Statuto dei lavoratori, malgrado il lifting operato con il già citato d.lgs. n. 151 del 2015, come lo stesso Regolamento UE 679 del 2016, ad oggi, non contemplano.
Invero, i dati derivanti dall'utilizzo di tali tecnologie non appartengono né alla sfera dei dati personali né a quella dei dati sensibili del lavoratore ma alla sfera dei dati che potrebbero essere definiti "sensibilissimi", sconosciuta al nostro ordinamento e al legislatore europeo.
Su tali presupposti, è evidente che i principi di necessità, correttezza, pertinenza e non eccedenza non saranno sufficienti a garantire la privacy del lavoratore ma si imporranno misure più incisive.
Le soluzioni potrebbero essere due. In primo luogo, per ogni azienda che tratterà dati *"sensibilissim*i" del lavoratore, potrà essere opportuno rendere obbligatoria la nomina di un Data Protection Officer. Come noto, ai sensi dell'art. 37 del Reg. UE 679 del 2016, ad oggi, tale figura è obbligatoria solo per soggetti pubblici o per le aziende ovvero per gli altri soggetti privati le cui attività principali consistono:
i) in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala, ii) ovvero che trattano, su larga scala, categorie particolari di dati o di dati personali relativi a condanne penali e reati.
Il *Data Protection Officer* dovrebbe vigilare perché l'utilizzo dei dati "sensibilissimi" dei lavoratori non violi le garanzie minime, in tema di diritto di lavoro e di privacy, a tutela degli stessi.
Ad esempio, nell'ottica dell'utilizzo di tali dati ai fini disciplinari, dovrebbe essere resa allo smart worker idonea informativa, nel senso del rischio del controllo dei suoi dati anche "sensibilissimi", con espressa accettazione dello stesso. E ciò sulla scorta di un modello già tracciato, sotto altri profili, dal d.lgs. n. 81 del 2008, accetta di correre o ancora, dovrebbe consentirsi allo *smart worker* il diritto di opporsi, con adeguato contradditorio, al trattamento dei dati "sensibilissimi" sulla scorta del diritto di

opposizione già contemplato, rispetto ai processi decisionali automatizzati, dall'art. 21 del Re. Ue 679 del 2016.
E così, sul piano pratico, il lavoratore dovrà essere messo nelle condizioni di provare che un errore commesso sul posto di lavoro che la tecnologia registra connesso ad un calo di produttività è conseguenza, non già di un volontario calo di produttività, ma di un particolare momentaneo stato di salute o della fisiologica stanchezza legata ad attività lavorativa intensiva.
Per intenderci sulla fallibilità di queste tecnologie, basti osservare quelle di molte auto di moderna generazione che segnalano al conducente cali dell'attenzione alla guida in conseguenza del semplice variare della velocità del veicolo, dovuto alle frequenti decelerazioni o frenature che il conducente, viceversa, prudentemente realizza in conseguenza delle code di auto o di alcuni ostacoli sui tratti stradali.
In secondo luogo, nel segno del principio di *by design*, potrebbe imporsi ai costruttori delle tecnologie in grado di leggere i dati "sensibilissimi" del lavoratore di adottare algoritmi intelligenti, anche attraverso il *machine learning*, in grado di interpretare tali dati e di trasmetterli solo ove necessario.
Uno spiraglio per nuove soluzioni a problemi nuovi sembra essere aperto, non a caso, dallo stesso Reg. Ue 679 del 2016 ove sia nel considerando n. 155 sia all'art. 88 rimette agli Stati membri il compito di elaborare, "*con legge o tramite contratti collettivi, norme più specifiche per assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro, in particolare per finalità di assunzione, esecuzione del contratto di lavoro, compreso l'adempimento degli obblighi stabiliti dalla legge o da contratti collettivi, di gestione, pianificazione e organizzazione del lavoro, parità e diversità sul posto di lavoro, salute e sicurezza sul lavoro, protezione della proprietà del datore di lavoro o del cliente e ai fini dell'esercizio e del godimento, individuale o collettivo, dei diritti e dei vantaggi connessi al lavoro, nonché per finalità di cessazione del rapporto di lavoro*"

Conclusioni

In conclusione, la tecnologia pone il nostro ordinamento dinanzi a nuove sfide che, per essere superate, richiedono ai *decision makers* di guardare alla realtà con lenti nuovi, dismettendo quelle novecentesche, e buone dose di ingegneria legislativa e contrattuale.
Ciò al fine di governarla indirizzandone il flusso. D'altro canto, significherebbe commettere un grave errore approntare paletti per arrestare la travolgente "piena" dell'innovazione.
Si tratta di applicare categorie giuridiche nuove a situazioni giuridiche nuove. In fondo, il cambiamento ci chiama a costruire una società win win in cui innovazione, lavoro e uomo vincono insieme.

Nota1 - Non a caso, la Relazione Ministeriale al disegno di legge dello Statuto dei lavoratori già ammoniva che la sorveglianza dovesse essere "mantenuta in una dimensione umana e cioè non esasperata dall'uso delle tecnologie che possono rendere la vigilanza stessa continua e anelastica, eliminando ogni zona di riservatezza e di autonomia nello svolgimento del lavoro".
Nota2 - Successivamente, è intervenuto il d.lgs. 185 del 2016, c.d. decreto correttivo, in modifica del d.lgs. n. 151 del 2015
Nota3 - Si vedano, per un approfondimento, le Linee Guida del Garante per la protezione dei dati personali n. 13 del 1 marzo 2017 in tema di utilizzo della posta elettronica e della rete internet aziendali.