

IL CONTROLLO A DISTANZA DEI LAVORATORI: IL JOBS ACT RISCRIVE L'ART. 4 L. 300/1970

di Giorgia Michela DE SANCTIS*

Sommario: 1. La disciplina del controllo a distanza nello Statuto dei lavoratori. 2. Nuove esigenze, nuovi profili di tutela, il Jobs Act. 3. La Cassazione sul controllo difensivo occulto mediante i social networks. 3.1. Uno sguardo oltre: la giurisprudenza penale ed il controllo effettuato mediante personale esterno all'attività aziendale. 4. Conclusioni.

1. La disciplina del controllo a distanza nello Statuto dei lavoratori

L'istituto del controllo a distanza dei lavoratori, negli ultimi anni, ha dovuto confrontarsi con l'introduzione e l'utilizzo nel mondo del lavoro di nuovi strumenti, altamente sofisticati dal punto di vista informatico, i quali seppur utili a rendere più efficace e veloce la prestazione lavorativa, risultano essere portatori di nuovi interrogativi riguardo i limiti e le condizioni di liceità

* Praticante avvocato

del controllo a distanza sui dipendenti.

La sempre attuale esigenza di contemperare le ragioni dell'impresa con il diritto alla riservatezza del lavoratore, ha reso necessario aggiornare una disciplina cardine, quale quella dello Statuto dei lavoratori, introduttiva nel nostro ordinamento della specifica tutela della riservatezza del lavoratore, adeguandola alla realtà di internet, della sorveglianza di massa e dei nuovi strumenti informatici.

La legge n. 300/1970, al titolo I "Della libertà e dignità del lavoratore", art. 4 "Impianti audiovisivi" co. I, prevedeva un

divieto assoluto dell'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dei lavoratori. Al comma successivo una parziale deroga permetteva l'installazione di detti impianti, qualora fossero richiesti da esigenze organizzative e produttive o dalla sicurezza del lavoro, pur se da questi fosse derivata la possibilità di controllo a distanza, subordinandone necessariamente l'installazione al previo accordo con le rappresentanze sindacali aziendali, o in mancanza di queste, con la commissione interna. A conferma di ciò, la suprema Corte afferma: "L'assenso delle Rsa è previsto per legge come uno dei momenti essenziali alla procedura sottesa all'installazione degli impianti ai sensi del secondo comma dell'art. 4".

2. Nuove esigenze, nuovi profili di tutela, il Jobs Act

Interessante notare come ad oggi, l'avvento dell'informatica nel mondo del lavoro, abbia influito sulle caratteristiche stesse del controllo, il quale risulta essere finalizzato all'efficienza della prestazione lavorativa, strettamente connessa all'utilizzo dei nuovi strumenti.

L'art. 23 del Jobs Act¹ - d.lgs. n. 151/2015- sostituisce integralmente l'art. 4 S.l. In prima battuta rievoca il testo del vecchio articolo, confermando la necessità dell'accordo sindacale per l'installazione di impianti audiovisivi e di altri strumenti dai quali derivi anche la possibilità di controllo a distanza, se giustificati da esigenze organizzative e produttive, per la sicurezza del lavoro, andando però ad aggiungere, *ex novo*, tra tali finalità, "la tutela del patrimonio aziendale", utile appiglio per la legittimazione dei controlli c.d. *difensivi occulti*.

¹ Art 23, d.lgs. 14 settembre 2015, n. 151, Disposizioni di razionalizzazione e semplificazione delle procedure e degli adempimenti a carico di cittadini e imprese e altre disposizioni in materia di rapporto di lavoro e pari opportunità, in attuazione della legge 10 dicembre 2014, numero 183, pubblicato in G.U. n. 221 del 23 settembre 2015.

Di seguito, una netta inversione di marcia, in quanto la disposizione di cui al comma I - riguardante la necessità dell'accordo sindacale - non verrà applicata agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze. In altre parole, strumenti di lavoro come pc, tablet, cellulari aziendali, potranno essere oggetto diretto di controllo a distanza, in quanto privati della garanzia del previo accordo sindacale. Continuando, le informazioni così raccolte saranno utilizzabili a tutti i fini connessi al rapporto di lavoro, nel rispetto di un'unica condizione, che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e dell'effettuazione dei controlli, unitamente al rispetto delle disposizioni del d.lgs. n. 196/2003 c.d. Codice Privacy².

L'aver "liberalizzato" gli strumenti utili a rendere la prestazione, sdoganando il loro controllo dal previo accordo sindacale, mina il diritto alla privacy del lavoratore, esponendo a rischio la sua sfera personale, affettiva, relazionale, senza contare l'aspetto della protezione dei propri dati personali, contingenti all'adempimento della prestazione.

Sorgono nuovi profili di tutela, si consideri "l'identità digitale del lavoratore",

² L'art. 1 del Codice Privacy riconosce a chiunque il diritto alla protezione dei dati personali che lo riguardano - il datore di lavoro che intenda effettuare un'attività di controllo del proprio patrimonio aziendale, che si risolva in un'attività di controllo a distanza dei propri dipendenti, riveste il ruolo di titolare del trattamento dei dati personali dei propri dipendenti. Egli deve trattare tali dati nella misura meno invasiva possibile, nel rispetto dei principi fondamentali in materia di trattamento di dati personali e svolgere attività di monitoraggio solo mediante i soggetti appositamente autorizzati, evitando un'ingiustificata interferenza sui diritti e sulle libertà fondamentali degli stessi. Gli obblighi imposti dal Codice privacy si costituiscono nella necessità di rispettare i 'principi di diritto' quali: il principio di necessità, il principio di proporzionalità ed il principio di finalità, in aggiunta al rilascio dell'informativa ai dipendenti ad alla prestazione del consenso da parte degli stessi. Cfr. Provvedimento del Garante per la protezione dei dati personali del 23 novembre 2006, Linee-guida per il trattamento di dati dei dipendenti privati.

il quale utilizzando gli strumenti aziendali, involontariamente o senza adeguata consapevolezza - si pensi anche ai lavoratori con una certa anzianità di servizio alle spalle, non dotati di grande dimestichezza con questi nuovi strumenti, i quali spesso necessitano di chiarimenti da figli e nipoti - lasci inevitabilmente traccia dei propri pensieri, delle proprie idee, gusti, del proprio orientamento politico o informazioni su dati di natura sensibilissima quali quelli inerenti all'ambito sanitario o riguardanti le preferenze sessuali, fornendo, malauguratamente, materiale utile ad eventuali condotte di mobbing.

Di contro sussiste l'interesse del datore di lavoro al corretto adempimento della prestazione lavorativa da parte del dipendente, per il quale tali strumenti, se usati impropriamente, possono rappresentare "motivo di distrazione" mettendo a rischio il corretto funzionamento degli impianti e dunque l'integrità del patrimonio aziendale.

Proprio la "tutela del patrimonio aziendale", viene esplicitata *ex novo*, rispetto all'art.4 S.l., tra le finalità dell'art. 23 del Jobs Act in forza dell'introduzione del nuovo inciso, al primo comma, che la riguarda. Ciò induce a porre l'attenzione sull'accertamento di eventuali comportamenti illeciti tenuti dal lavoratore e conseguentemente sulla legittimità del *controllo difensivo occulto*, operato dal datore di lavoro.

3. La Cassazione sul controllo difensivo occulto mediante i social networks

La sentenza n.10955/2015 ha affermato il principio di generale ammissibilità dei controlli difensivi occulti, purché diretti ad accertare comportamenti illeciti diversi dal mero inadempimento della prestazione lavorativa ed effettuati mediante modalità non eccessivamente invasive, ma rispettose, delle garanzie di dignità e riservatezza del lavoratore, nell'osservanza dei canoni generali di buona fede e correttezza contrattuale.

Nella fattispecie, un operaio addetto

alle presse stampatrici era stato licenziato per giusta causa in seguito a varie condotte tenute. Si era allontanato dalla sua postazione per una telefonata privata che gli aveva impedito di intervenire prontamente su di una pressa bloccata da una lamiera, incastratasi tra i meccanismi; era stato trovato nel sul armadietto aziendale un I-pad acceso ed in collegamento con la rete elettrica aziendale e successivamente si era intrattenuto a conversare su Facebook, mediante cellulare.

La particolarità del caso risiede nella modalità di accertamento del fatto, reso possibile mediante la creazione da parte del responsabile del personale, su autorizzazione del datore di lavoro, di un "*falso profilo di donna su Facebook*". L'intento alla base di quest'escamotage consisteva nell'approcciare il lavoratore, incentivando lo sviluppo della conversazione telematica tra i due soggetti, non per dimostrare un semplice inadempimento della prestazione lavorativa, ma che mediante tale distrazione, sommata alle altre, era stato esposto a rischio il patrimonio aziendale. E dunque, la Corte ha rigettato il ricorso proposto dal lavoratore, statuendo che "lo stratagemma" adoperato dall'azienda per accertare le sue conversazioni telefoniche via internet, durante l'orario di lavoro, non costituisce una forma di controllo a distanza, vietata dal novellato art. 4, ma una forma di controllo destinato a riscontrare e sanzionare un comportamento idoneo a ledere il patrimonio aziendale, sotto il profilo del regolare funzionamento e della sicurezza degli impianti.

3.1 Uno sguardo oltre: la giurisprudenza penale ed il controllo effettuato mediante personale esterno all'attività aziendale

Da segnalare è anche il profilo della *localizzazione del dipendente* all'interno dei locali aziendali, avvenuta in conseguenza all'accesso Facebook da cellulare.

È principio affermato dalla giurisprudenza penale che l'attività d'indagine volta a seguire i movimenti di un soggetto e a localizzarlo, controllando a distanza la sua pre-

senza in un dato luogo e momento mediante GPS, costituisce una forma di pedinamento eseguito con strumenti tecnologici, non assimilabile ad attività d'intercettazione, così come prevista dall'art. 266 c.p.p. e ss.³, ma piuttosto ad *un'attività di investigazione atipica*⁴, i cui risultati potrebbero senz'altro essere utilizzati in sede di formazione del convincimento del giudice⁵. Il che amplia lo scenario futuro, legittimando i controlli effettuati mediante personale esterno all'attività aziendale, si pensi all'ipotesi per la quale il datore di lavoro si serva di un'agenzia investigativa⁶.

4. Conclusioni

La disposizione dell'art. 4 della legge n. 300/1970 a tutela della riservatezza dei lavoratori, era stata formulata sulla base dei pochi strumenti di controllo esistenti, principalmente gli impianti audiovisivi e di video sorveglianza. Il legislatore degli anni '70 non poteva prevedere lo sviluppo epocale che avrebbe avuto l'informatica e soprattutto l'azione di contaminazione che questa

avrebbe esercitato su aspetti sensibili della prestazione resa dal dipendente. Ad oggi, lo spazio entro il quale il lavoratore opera, non è più solo quello dei locali dell'azienda o quello delimitato dalle quattro mura del suo ufficio, ma l'immenso mondo telematico. Sorgono nuove fattispecie bisognevoli di tutela, al divieto del controllo a distanza continuo ed anelastico previsto nello Statuto dei lavoratori, si aggiunge l'esigenza di tutelare il lavoratore nel momento in cui l'adempimento della sua prestazione richiede l'utilizzo di strumenti, spesso a lui poco familiari, il cui uso conscio diventa fondamentale. Specularmente si pone l'interesse del datore di lavoro al corretto adempimento della prestazione da parte dei dipendenti, nell'ipotesi in cui questi possano lasciarsi distrarre da un uso distorto ed improprio degli stessi, andando a ledere il patrimonio aziendale.

Al fine di poter contemperare al meglio il diritto alla privacy del lavoratore con quello alla tutela del patrimonio aziendale del datore di lavoro, sarebbe auspicabile uno studio accurato e minuzioso delle Policy di utilizzo di tutti gli strumenti di lavoro funzionali alle mansioni dirette ed accessorie del personale dipendente, finalizzato ad un uso conscio, consapevole e corretto, risultando coerenti al nuovo scenario generato dalla novella dell'art. 4, nell'interesse di entrambe le parti.

³ Cass. pen. Sez. II, 13 febbraio 2013, n. 21644.

⁴ Cass. pen. Sez. IV, 27 novembre 2012, n. 48279.

⁵ Cfr. sull'ammissibilità delle prove atipiche Cass. civ. Sez. II, 5 marzo 2010, n. 5440.

⁶ Cass. civ. Sez. lav., 10 luglio, 2009 n. 16196.

Abstract

L'art. 23 del d.lgs. n. 151/2015 sostituisce integralmente l'art. 4 della l. n. 300/1970, per un verso confermando aspetti della disciplina del controllo a distanza, riguardanti l'installazione degli impianti audiovisivi e di video sorveglianza, per un altro innovando tale disciplina, menzionando i nuovi strumenti informatici utili a rendere la prestazione, il controllo dei quali viene privato della garanzia del previo accordo sindacale, lasciando presagire la difficile ricerca di un punto di equilibrio tra la tutela della privacy del lavoratore e l'interesse all'efficienza della prestazione da parte del datore di lavoro, prospettando nuove fattispecie bisognevoli di tutela, legate all'invasivo avvento dell'informatica nel mondo del lavoro.

The art. 23 of d.lgs. 151/2015 replaces art. 4 of law n. 300/1970, confirming aspects of the discipline of remote control already "run", relating to the installation of audiovisual equipment and video surveillance, for another innovating such discipline, mentioning the new it tools useful in making the provision, the control of which is deprived of the warranty of the Union agreement, leaving portend the difficult search for a balance between the protection of privacy of the worker and the interest to the efficiency of the performance by the employer, proposing new case needprotection, related to invasive advent of computers in the workplace.