LavoroDirittiEuropa
Rivista nuova di Diritto del Lavoro

Numero 3 / 2020

(estratto)

Gabriele Consonni

Commento al paragrafo "*Il Grande Fratello e il lavoro*" facente parte del saggio "*Il manifesto per un diritto del lavoro sostenibile*" di Caruso, Del Punta, Treu

Commento al paragrafo "*Il Grande Fratello e il lavoro*" facente parte del saggio "*Il manifesto per un diritto del lavoro sostenibile*" di Caruso, Del Punta, Treu

Gabriele Consonni

Avvocato presso il Foro di Pavia

Dottore di ricerca in diritto del lavoro presso l'Università degli Studi di Pavia

L'individuazione della normativa in materia di privacy come argine principale della tutela del dipendente sul posto di lavoro concretizzata dall'art. 23 D.lgs. 151/2015, tale da "*scacciare lo spettro di Grandi Fratelli insediati nelle aziende*" come suggerito dagli Autori, rappresenta un punto di partenza non completamente innovativo se si considera che, alla luce di quanto disposto dall'art. 171 D.lgs. 196/2003[1] nella versione vigente fino al 24 settembre 2015, la violazione dell'art. 4 dello Statuto dei Lavoratori era punita con le sanzioni penali di cui all'art. 38 Stat. Lav.: è già da quindici anni, dunque, che è possibile individuare tracce della volontà del Legislatore di intrecciare, da un lato, le norme finalizzate alla protezione dei dati personali e, dall'altro, le istanze di tutela della figura del lavoratore rispetto al potere di controllo imprenditoriale nell'ambito del contesto aziendale.

La vera novità espressa con il *Jobs Act* va individuata, semmai, nell'esplicito richiamo già all'interno dell'art. 4 Stat. Lav. (e non più, come in passato, solo nelle disposizioni finali dello Statuto dedicate all'impianto sanzionatorio applicabile in caso di violazioni) del ruolo centrale dell'informativa (adeguata) da fornire ai dipendenti circa le modalità di estrinsecazione del potere di controllo nel rispetto dei principi fondamentali in materia di trattamento dei dati personali, la cui disciplina è oggi essenzialmente contenuta nel Regolamento (UE) 2016/679 (cd. GDPR); un rinvio che non può evidentemente essere oggetto di un'interpretazione meramente letterale (considerato che il comma 3 della disposizione richiama espressamente solo il D.lgs. 196/2003, testo ormai diventato di secondo piano quale disciplina in materia di protezione dei dati personali) come limitato agli strumenti cosiddetti di *hard law* (quali le norme cogenti di matrice europea e nazionale), ma destinato a gettare luce pure sugli interventi di *soft law* rilevanti per la materia in esame. Mi riferisco, in particolare, al Parere 2/2017 elaborato dal Gruppo di Lavoro Articolo 29 (sostituito, a seguito all'entrata in vigore del GDPR, dal Comitato Europeo per la Protezione dei Dati Personali), contenente svariate indicazioni finalizzate a consentire un corretto trattamento dei dati personali

[1] TROJSI, *Controllo a distanza (su impianti e strumenti di lavoro) e protezione dei dati del lavoratore*, in Var. tem. Dir. Lav., 2016, IV., pp. 684-685.

dei dipendenti all'interno del contesto lavorativo: dall'opportunità di evitare l'utilizzazione del consenso del lavoratore come base legale per il trattamento (alla luce della palese condizione di ontologica disparità tra la figura datoriale e quella del prestatore, con conseguente sussistenza dei legittimi dubbi circa la genuinità del consenso espresso[2]), alla conformità piena al principio di trasparenza di cui all'art. 5 GDPR ("*i dipendenti devono essere informati in maniera chiara e completa del trattamento dei loro dati personali, ivi compreso dell'esistenza di qualsiasi monitoraggio*" […] "*i dipendenti devono essere informati dell'esistenza di qualsiasi monitoraggio, delle finalità per le quali i dati personali devono essere trattati e deve essere fornita loro ogni altra informazione necessaria per garantire un trattamento lecito. Con l'avvento delle nuove tecnologie, la necessità di trasparenza diventa più evidente in considerazione del fatto che tali tecnologie consentono la raccolta e l'ulteriore trattamento in maniera occulta di volumi potenzialmente enormi di dati personali"*), alla presa di consapevolezza delle immense potenzialità di controllo di cui sono dotate le tecnologie moderne sempre più spesso impiegate sul luogo di lavoro[3], con il conseguente oltremodo concreto rischio che il legittimo interesse dell'imprenditore ad un organizzazione aziendale più efficiente e produttiva possa avere come effetto concreto quello di instaurare un sistema di monitoraggio costante e troppo largamente pervasivo, tale comunque da dissuadere i dipendenti dall'esercizio dei propri diritti quali, ad esempio, il diritto di critica o il diritto di espressione della propria personalità all'interno del contesto aziendale. Va da sé che, ovviamente, l'esercizio di tali diritti andrà comunque mantenuto entro limiti ben definiti, tali comunque da non configurare un grave inadempimento agli obblighi derivanti dagli artt. 2094 e ss. c.c. e dal contratto individuale di lavoro, legittimante l'irrogazione di una sanzione disciplinare se non addirittura del licenziamento; d'altra parte, è superfluo ricordare come la funzione primaria dello Statuto dei Lavoratori fosse essenzialmente quella di consentire finalmente l'ingresso dei principi costituzionali pure all'interno del contesto aziendale[4].

D'altro canto, la volontà di dare "*corpo a un'idea di civiltà dei controlli informatici sul lavoro, ispirata a un pragmatico bilanciamento tra le esigenze datoriali e la sfera personale del lavoratore*" individuata dagli Autori

[2] Si veda *funditus* l'art. 7, paragrafo 4, GDPR, a mente del quale il consenso deve essere liberamente prestato, nonché il Considerando 43 del Regolamento: è opportuno che il consenso non costituisca un valido fondamento giuridico per il trattamento dei dati personali in un caso specifico, qualora esista un evidente squilibrio tra l'interessato e il titolare del trattamento.

[3] Con particolare riferimento all'importanza assunta dai cd. *wereable devices* (una sorta di computer in miniatura indossabili dai dipendenti e perennemente connessi col contesto informatico aziendale, utilizzati principalmente per consentire un efficientamento delle prestazioni lavorative rese -si pensi al caso emblematico del braccialetto elettronico ipotizzato da Amazon-) si veda *funditus* INGRAO, *Il braccialetto elettronico tra privacy e sicurezza del lavoratore*, Dir. Rel. Ind., 2019, pp. 895 e ss.

[4] RODOTÀ, *Tecnologia e diritti*, Il Mulino, Bologna, 1995, ha evidenziato come le regole poste dallo Statuto dei Lavoratori (in particolar modo l'art. 8) abbiano rappresentato la prima vera innovazione in tema di protezione delle informazioni, di fatto anticipando di venticinque anni sia la normativa comunitaria che la L.n. 675/1996, prima attuazione nell'ordinamento italiano della Direttiva 95/46 CE. Secondo GRAGNOLI, *Dalla tutela della libertà alla tutela della dignità e della riservatezza dei lavoratori*, in Arg. dir. lav., 2007, p. 1211, in Italia la tutela del diritto alla riservatezza avrebbe trovato ingresso proprio "*attraverso il portone dello Statuto*".

sembra, al momento, essere stata accolta da parte della giurisprudenza: "*L'art. 4 St. Lav. stabilisce che le apparecchiature dalle quali possa derivare il controllo a distanza del lavoratore debba essere autorizzato, e condiziona l'utilizzabilità dei dati acquisiti all'avvenuta "adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli" nei confronti dei lavoratori. Ciò detto, non è sufficiente per ritenere rispettata tale previsione la circostanza che i lavoratori fossero a conoscenza della presenza di telecamere, dovendo l'informazione essere estesa alle modalità d'uso dei dati acquisiti ivi compresa, soprattutto, la possibilità di effettuare controlli sulla prestazione lavorativa*" (Trib. Venezia 23 luglio 2020); "*i controlli eseguiti dal datore di lavoro contrastano con il comma 3 dell'art. 4 L. 300/1970, qualora il lavoratore non sia stato adeguatamente informato né sulla concreta possibilità, né tanto meno sulle modalità relative a eventuali controlli da parte del datore di lavoro sul proprio computer e sulla propria e-mail aziendale*" (Trib. Vicenza 28 ottobre 2019); "*viola la normativa sulla privacy il datore di lavoro che controlla il dipendente disponendone il pedinamento e l'accesso all'account di posta elettronica senza dare atto delle ragioni e delle effettive modalità del controllo. Non può essere configurato come legittimo ai sensi dell'art. 4, comma 2 st. lav. il controllo effettuato sull'account email del dipendente in assenza dell'adeguata informazione prevista dall'art. 4, comma 3 st. lav. Le predette violazioni comportano l'inammissibilità delle risultanze ottenute dai controlli occulti e, dunque, l'inutilizzabilità delle informazioni acquisite*" (Trib. Milano 13 maggio 2019).

Relativamente poi al profilo specifico della tutela della dignità dei dipendenti e al pericolo di utilizzabilità, da parte del datore di lavoro, di informazioni e dati facilmente reperibili su Internet e sui *social media*, è ancora una volta utile prendere le mosse dallo spunto fornito dal Parere 2/2017 del Gruppo di Lavoro Articolo 29: il datore di lavoro non dovrebbe ritenersi libero di utilizzare le informazioni dei propri dipendenti (ovvero dei candidati a ricoprire una posizione lavorativa nella propria azienda) presenti su Internet solo in quanto liberamente accessibili da qualunque internauta, essendo suo onere innanzitutto valutare l'eventuale sussistenza di un proprio legittimo interesse a tale tipologia di trattamento ai sensi dell'art. 7, lett. f), GDPR e, in secondo luogo, di considerare se il profilo Internet del candidato/dipendente sia stato creato appositamente per trovare una posizione lavorativa (si pensi al caso di LinkedIn) oppure per scopi personali (si pensi ai profili *social* di Instagram e Facebook), ciò rappresentando un indice fondamentale onde valutare la liceità del trattamento posto in essere.

Nei prossimi anni sarà dunque importante che le imprese acquisiscano sempre maggiore consapevolezza dell'obbligo di adozione di comportamenti *GDPR friendly* (anche alla luce delle sempre più ingenti sanzioni economiche che le varie autorità garanti stanno irrogando in questi mesi nei confronti dei titolari che violino le disposizioni della normativa *privacy*), onde evitare che davvero il potere di controllo si consolidi nella figura di un Grande Fratello deputato a sorvegliare ogni istante della vita lavorativa (ma non solo) del dipendente.