LaBoUR & Law Issues
Rights | Identity | Rules | Equality

Il controllo a distanza realizzato mediante Social network

ALESSANDRA INGRAO
Università degli Studi di Milano

vol. 2, no. 1, 2016

ISSN: 2421-2695

LaBoUR & Law Issues
Rights | Identity | Rules | Equality

Il controllo a distanza realizzato mediante Social network

ALESSANDRA INGRAO
Università degli Studi di Milano
alessandra.ingrao@gmail.com

ABSTRACT

The Author focuses on the recently reformed provisions regulating the employer's power to control from remote the employees' activities (art. 4 of the Workers Statute), with particular regard to controls performed by means of Social networks.
Such controls are in fact extremely powerful due to the versatile and multi-purpose character of Social networks, which may also be used as a working device. A widespread case law shows indeed that employer's controls may cost a worker his job
Therefore, after the reform, all employees will have to read carefully the employer's Privacy policies, before accessing socials during the worktime to express opinions and/or frustrations.

Keywords: Social network - Web 2.0 – Social media marketing – Employer's monitoring power – Data protection - Employee's privacy.

Il controllo a distanza effettuato mediante Social network

SOMMARIO: 1. Le peculiarità dei Social network identificativi e le loro potenzialità di controllo a distanza dell'attività lavorativa e del comportamento dei lavoratori - 2. Il vecchio art. 4 St. lav. alla prova dei Social network - 3. Il nuovo art. 4 St. lav.: come si cambia per non morire - 4. Il nuovo art. 4 e i Social network. Quando il Social è strumento di lavoro - 5. *Segue*. quando il Social è strumento di controllo

1. Le peculiarità dei Social network identificativi e le loro potenzialità di controllo a distanza dell'attività lavorativa e del comportamento dei lavoratori.

«Non molto tempo fa, in una terra lontana, esisteva un sistema di editori feudali. Questi editori cercavano di controllare il numero maggiore di utenti. Gli archeologi avrebbero definito quest'era preistorica web 1.0. Gli utenti, per un po' di tempo, furono felici, fino al giorno in cui scoprirono che anche loro potevano diventare degli editori facilmente e formare le proprie comunità e i propri regni. Crearono così una nuova terra nella quale i contenuti erano democratici e dove ogni utente avrebbe potuto divenire il re di se stesso. I nuovi siti consentirono ben presto agli utenti di pubblicare i loro decreti reali (blog), votare per i contenuti, trovare vecchi amici, diventare star, avere dei seguaci e in taluni casi diventare anche più potenti dei vecchi editori. Gli utenti chiamarono questa nuova Utopia web 2.0. Benvenuti nel Social web» (1).

I Social network, nell'inarrestabile ascesa che li ha visti coinvolti, sono stati in grado di travalicare le porte delle fabbriche, degli uffici e, più in generale, dei luoghi di lavoro. Il web 2.0, grazie alle sue numerose funzionalità, è divenuto una delle numerose tecniche di controllo a distanza sul comportamento del lavoratore-utente.

Due semplici operazioni permettono al lavoratore di essere controllato sui Social network: la creazione di un profilo identificativo (pubblicazione di contenuti e personalizzazione) (2) e la partecipazione (interazione) attiva ad una *societas* virtuale.

(1) F. Mini, *Social Media. Introduction*, in R. Ford, J. Wiederman (edited by), *Internet Case Study Book*, Taschen, 2010, 232.

(2) Si distingue in letteratura tra network, il cui funzionamento presuppone che l'utente riveli la propria identità sia agli altri utenti che al gestore in senso verticale (cd. identificativi) e network che non necessitano di questa identificazione. La distinzione oltre a rilevare a livello di struttura logica del programma (che individua il modo in cui la rete può influire sugli utenti e il modo in cui essi possono interagire tra

Il fruitore del web esce dal triste anonimato della vita quotidiana e rivela al gestore del network e agli altri utenti la propria identità, i propri gusti (*like*), le proprie opinioni (*post* e *tweet*), la propria storia personale e, addirittura, i propri comportamenti in tempo reale. Ciascun utente, nell'ecosistema cibernetico, possiede una vita autonoma, interagisce con gli altri fruitori della rete e si ritaglia un ruolo nella società digitale.

Tutto questo è possibile grazie alle innumerevoli funzioni tecnologiche che i Social mettono a disposizione: supporto per pubblicare immagini, video e commenti, servizio di messaggistica in tempo reale (*chat*), geolocalizzazione (*check-in*) ed individuazione dell'orario in cui ciascuna azione virtuale viene compiuta.

Se, quindi, all'interno del Social, l'utente possiede un'esistenza virtuale, è altrettanto vero che di tutte le azioni da questo poste in essere nella piattaforma rimane traccia all'interno del supporto digitale, fornito dal *provider* del servizio (3). Tracce che, nel linguaggio del legislatore, si chiamano dati personali e dati sensibili, meritevoli di protezione giuridica perchè idonei a dischiudere informazioni che potrebbero contribuire a compromettere la stabilità del rapporto di lavoro (4).

Tuttavia, il problema che si trova a dover affrontare il lavoratore-utente non si esaurisce a questo aspetto. Perché questa vita virtuale, piena di sollecitazioni e di stimoli, può indurlo a dedicare tempo alla gestione della sua immagine sui Social anziché alla prestazione lavorativa che è obbligato, contrattualmente, a svolgere. Il Social diventa così un *divertissement* in orario e sul luogo di lavoro. E rappresenta una distrazione pericolosa per la conservazione del posto di lavoro, qualora il lavoratore, in spregio al dovere di diligenza di cui all'art. 2104 c.c., interrompa lo svolgimento della prestazione e abbandoni le macchine aziendali per

---

loro), appare fondamentale per l'applicazione della disciplina di *data protection,* poiché solo con riferimento ai *network identificativi* si avverte l'esigenza di tutelare le informazioni personali degli utenti.

(3) I Social network sono servizi offerti da società operanti su scala mondiale per consentire alle persone di interagire virtualmente tra loro. Secondo la Direttiva 98/34/CE, i fornitori sono inquadrabili giuridicamente tra i servizi della società dell'informazione. Se poi, come normalmente accade, il Social è idoneo a fornire servizi di comunicazione elettronica, cioè consente all'utente di inserire contenuti da lui stesso creati (foto, testi e musica), ad esso devono essere applicate anche le disposizioni della Direttiva 2002/58/CE concernente la vita privata e le comunicazioni elettroniche.

(4) Per un'analisi delle tutele previste dall'art. 8 St. lav. si consenta di rinviare a F. Iaquinta, A. Ingrao, *La privacy e i dati sensibili del lavoratore legati all'utilizzo di social networks. Quando prevenire è meglio che curare*, *DRI*, 2014, 1027. Senza approfondire il tema in questa sede un caso per tutti può far riflettere: *Snyder* v. *Millersville Univ*., No. 071660, 2008 U.S. Dist. LEXIS 97943, at 12-22 (E.D. Pa Dec. 3, 2008), ove si trattava di una maestra elementare ritratta ubriaca in una fotografia postata su *My Space,* la quale è stata licenziata perché ritenuta inadatta a svolgere servizi educativi.

dedicarsi all'attività di *chat* con una bella signora (5) o per affrontare le sfide che gli amici gli lanciano sulle *app* scaricate. Pericolosa in quanto il tempo sottratto all'attività lavorativa si traduce in mancata produttività di uno dei fattori che compongono l'organizzazione aziendale.

Ma la vita sui Social permette al lavoratore di fare di peggio. Esattamente come nella vita reale, il prestatore di lavoro può assumere comportamenti illeciti (6). E, così, anche l'illecito, nell'era della tecnologia, si digitalizza. La casistica (7) giurisprudenziale indica che, mediante un banale *click*, il patrimonio aziendale, inteso soprattutto in un'accezione ampia, comprensivo di beni immateriali (quali l'immagine aziendale presso la clientela messa a rischio dalle offese dei lavoratori, i segreti industriali e il *know-how* rivelati grazie a fotografie postate su Facebook) subisce gravi lesioni che portano il datore di lavoro a considerare "spezzato" quel vincolo fiduciario che lo legava al singolo dipendente.

In risposta a questa svariata gamma di comportamenti illeciti ed inadempienti (8) che il lavoratore può manifestare sul Social, il creditore

(5) Cfr. il noto caso giudicato da Cass. 27 maggio 2015, n. 10955 *FI*, 2015, I, 2316, secondo cui è legittimo il controllo a distanza, effettuato mediante la creazione di un profilo *fake* di Facebook per indurre il lavoratore all'attività di *chat*; quando tale controllo sia volto ad accertare un comportamento «lesivo del patrimonio aziendale, sotto il profilo del regolare funzionamento e della sicurezza degli impianti».

(6) Si tratta di comportamenti «idonei a ledere il patrimonio aziendale, i beni aziendali e tutti quei beni estranei al rapporto di lavoro», cfr. Cass. 3 aprile 2002, n. 4746, *RGL*., 2002, 642 e in *MGL*., 2002, 644, nt. Bertocchi; Cass. 17 luglio 2007, n. 15892, in *RGL*, 2008, 358 e in *RIDL*, 2008, 714, nt. Vallauri; Cass. 23 febbraio 2010, n. 4375, in *RIDL*, 2010, II, 564; Cass. 23 febbraio 2012, n. 2722, *FI*, 2012, I, 1421; Cass. 1 ottobre 2012, n. 16622, *FI*, 2012, I, 3328.

(7) Nella Relazione del Garante Privacy per il 2010, a p. 112, è segnalato il caso di un lavoratore licenziato a causa dell'utilizzo di Facebook: il dipendente aveva pubblicato nel proprio profilo visibile agli "amici degli amici" alcune foto scattate nei locali aziendali dove, sullo sfondo, erano visibili disegni coperti, secondo l'azienda, da segreto industriale. Tali prove venivano dichiarate acquisite lecitamente e conseguentemente utilizzabili perché il profilo del lavoratore era potenzialmente visibile da una cerchia indeterminabile di utenti (per l'appunto "gli amici degli amici"). Interessante appare, inoltre, il caso deciso da Trib. Milano, ordinanza, 1 agosto 2014, in *RIDL*, 2014, con nota di F. Iaquinta, A. Ingrao, *Il datore di lavoro e l'inganno di* Facebook; nel caso di specie il lavoratore, licenziato per giusta causa, postava sul proprio profilo Facebook "pubblico" alcune fotografie, scattate durante l'orario di lavoro, in circostanze di luogo e di tempo tali da provare l'allontanamento dal posto di lavoro e l'interruzione della prestazione. Peraltro le fotografie erano corredate da frasi ingiuriose quali «come si lavora bene alla A. srl di merda».

(8) Sin da subito giova rimarcare che esiste un'inscindibile connessione sul piano teorico tra attività illecita e comportamento inadempiente alle obbligazioni che la legge fa discendere dal contratto di lavoro. Cfr. P. Tullini, *Videosorveglianza a scopi difensivi e utilizzo delle prove di reato commesso dal dipendente*, *RIDL*, 2011, II, 89. L'Autrice

della prestazione sviluppa, sempre più frequentemente, il desiderio di sapere cosa "combina" il singolo lavoratore sulla piattaforma digitale. Non si tratta semplicemente di soddisfare una mera curiosità, ma talvolta viene in gioco l'esigenza di difesa del datore di lavoro, che spesso viene soddisfatta attraverso lo svolgimento di un'attività investigativa e di sorveglianza rivolta a scovare queste *bad practices,* nonché finalizzata ad incamerare risultanze probatorie da utilizzare in giudizio al fine di evitare che queste scorrettezze restino impunite.

La tecnologia del web 2.0 è certamente un potente alleato del controllante. Le sue caratteristiche tecniche, sopra esaminate, permettono di individuare da quale luogo e in quale fascia oraria l'utente è connesso, consentono di incamerare tracce, indizi e di procurarsi prove dell'adempimento o dell'inadempimento del lavoratore. E uno degli elementi più rilevanti, per chi la utilizza, è che il controllo ha un costo pari a zero e che l'utilizzo dei Social è facile e accessibile anche per il "*bonus prudens diligens pater familias*" di antica memoria. Non solo. I dati e le informazioni incamerati all'interno del Social, restano memorizzati nella piattaforma digitale, indipendentemente dal fatto che la persona si serva di un pc, *smartphone* o *tablet* di proprietà aziendale. Ed infatti, la funzione di controllo sul Social si attiva a prescindere dalla proprietà del *device* da cui si accede alla piattaforma.

L'evoluzione dei Social network, che perdono la loro funzione originaria di svago e divertimento, e diventano un temibile strumento di controllo, impone una riflessione. La domanda cui occorre dare risposta è se i dati reperibili sui Social network possano costituire fonti di prova utilizzabili in giudizio per contestare l'inadempimento o un fatto illecito al lavoratore. E, qualora la risposta alla prima domanda sia positiva, in quali limiti ciò è concesso dall'ordinamento.

Per dare soluzione a questo quesito occorre analizzare com'è cambiata l'architettura di regole su cui si regge la materia del controllo a distanza, a seguito della novella che ha interessato l'art. 4 St. lav.

2. Il vecchio art. 4 St. lav. alla prova dei Social network

Il legislatore del 1970, che certamente nel disciplinare la fattispecie del "controllo a distanza" non aveva considerato i Social network, ci aveva consegnato una norma che regolava, procedimentalizzandolo, il potere d'installazione di apparecchiature di controllo, qualora esse avessero consentito un controllo indiretto sull'attività lavorativa. La norma, inoltre, con la finalità di proteggere la dignità di chi lavora (9),

evidenzia che, nella maggior parte dei casi concreti, l'interferenza tra illecito ed inadempimento «esiste ed è ineliminabile».

(9) Peraltro, questa interpretazione strettamente letterale del previgente art. 4, comma 1, St. lav. era supportata da un'interpretazione sistematica. Il predetto art. 4

vietava in modo assoluto che l'adempimento della prestazione lavorativa e il rendimento del lavoratore fossero controllati esclusivamente "a distanza".

Il testo previgente, in particolare ruotava attorno a due punti fermi: l'oggetto materiale su cui il datore di lavoro poteva esercitare l'attività di osservazione e giudizio non poteva mai coincidere esclusivamente con "l'attività dei lavoratori" (art. 4, comma 1, St. Lav. nella versione previgente) (10). Nondimeno, se il datore di lavoro intendeva proteggere cautelativamente la sua organizzazione produttiva, intesa in senso lato, poteva procedere all'installazione di apparecchiature di controllo a distanza, anche se da queste avrebbe potuto derivare il controllo sull'attività lavorativa. Ma, si badi bene, la legittimità di questa scelta era condizionata al raggiungimento di un accordo sindacale (o in mancanza di questo, all'ottenimento di un'autorizzazione amministrativa) volto ad accertare l'effettiva presenza delle causali rappresentate da esigenze produttive, organizzative o di sicurezza, ritenute dal legislatore meritevoli di tutela, quindi capaci di giustificare oggettivamente l'installazione delle apparecchiature di sorveglianza. Inoltre, l'effettiva sussistenza di queste causali aveva la funzione di imprimere un "vincolo" di utilizzabilità agli esiti delle rilevazioni provenienti dagli strumenti installati. Si tendeva, in particolare, ad escludere la possibilità di utilizzare tali informazioni ad altri fini (es. disciplinari), diversi da quelli che ne avevano giustificato la legittima installazione (11).

---

era, ed è tuttora, collocato dopo l'art. 3 St. lav. (immutato dopo il *Jobs Act*) che disciplina il controllo svolto da persone fisiche sull'attività lavorativa, subordinandolo ad un principio di pubblicità e trasparenza. Nel raffronto tra le due norme è lampante che, in ragione delle caratteristiche e delle modalità con cui si svolge il controllo umano – che per sua natura avviene *vis-à-vis,* cioè in presenza (fisica) del sorvegliato, il quale si accorge di essere controllato – esso possa avere ad oggetto anche il corretto svolgimento dell'attività lavorativa. Mentre nel caso del controllo tecnologico, che si svolge a distanza sia di spazio che di tempo grazie a strumenti che sono in grado di immagazzinare flussi d'informazioni, memorizzarli e conservarli anche per lunghi periodi, il legislatore aveva vietato che l'imprenditore potesse mettere sotto il *Panopticon* o *Synopticon*, l'adempimento esatto dell'obbligazione lavorativa.

(10) L'interpretazione pressoché unanimemente condivisa della locuzione "attività dei lavoratori" era idonea ricondurre nell'ambito del divieto non solo controlli sui comportamenti strettamente strumentali all'adempimento dell'attività lavorativa, ma anche la sorveglianza su tutte quelle attività che esorbitano dal momento tecnico funzionale della subordinazione, denominate in dottrina "licenze comportamentali". Sul punto F. Liso, *Computer e controllo dei lavoratori*, *DLRI,* 1986, 366, 369; A. Garilli, *Tutela della persona e tutela della sfera privata nel rapporto di lavoro*, *RCDP*, 1992, II, 321.; P. Lambertucci, *Potere di controllo del datore di lavoro e tutela della riservatezza del lavoratore: i controlli a "distanza" tra attualità della disciplina statutaria, promozione della contrattazione di prossimità e legge delega del 2014 (c.d. Jobs act), CSDLE, It.,* n. 255/2015.

(11) Peraltro, nel vigore della vecchia norma, anche il diritto vivente andava in questa direzione. Gli accordi sindacali siglati ex art. 4 St. lav. e i provvedimenti

Il testo previgente dell'art. 4 St. lav. non conteneva alcuna indicazione circa la sorte delle informazioni raccolte in violazione dei limiti posti dal legislatore al potere di controllo a distanza. Ma questa lacuna normativa fu colmata dalla giurisprudenza che tradusse la "inutilizzabilità della prova" in una dichiarazione giudiziale di inammissibilità (12).

Tuttavia, se la norma costituiva una forte barriera per l'attività di osservazione e giudizio dello svolgimento dell'attività lavorativa e del rendimento del lavoratore, lo stesso non poteva affermarsi con riferimento a casi di comportamenti illeciti (anche di natura penale) perpetrati dai dipendenti. La norma (come del resto anche le disposizioni che disciplinano il controllo svolto con mezzi umani), infatti, presentava una rilevante criticità: non regolava in modo specifico l'ipotesi del controllo a distanza sui fatti illeciti dei lavoratori. Di conseguenza, la giurisprudenza (13) è intervenuta a colmare il predetto vuoto normativo, con riferimento alla tutela dell'impresa, mediante l'elaborazione di una categoria giuridica autonoma, i c.d. "controlli difensivi", con l'obbiettivo di svincolare il potere datoriale di controllo a distanza, di tipo reattivo, dalle maglie strette della procedura sindacale codeterminativa, attraverso la disapplicazione integrale dell'art. 4, con la finalità di restituire valore all' esigenza del datore di lavoro di difendersi da comportamenti illeciti dei propri dipendenti.

Sennonché, la criticata (14) teoria del controllo difensivo, oltre ad avere l'effetto di legalizzare controlli occulti, lesivi della dignità e della privacy del lavoratore, si scontrò con l'irrisolvibile problema della distinzione in concreto tra controllo dell'illecito, ammesso, e controllo dell'inadempimento contrattuale, vietato.

---

autorizzatori contenevano espressamente la clausola di inutilizzabilità delle informazioni a fini disciplinari. cfr. A. Bellavista, *Il controllo sui lavoratori*, Giappichelli Editore, 1995; U. Romagnoli, *Sub art. 8*, in G. Ghezzi, F. Mancini, L. Montuschi, U. Romagnoli, *Statuto dei diritti dei lavoratori*, Zanichelli, 1979.

(12) Si rinvia alla giurisprudenza citata nelle note successive, alla luce della quale, è possibile affermare che l'art. 4 St. lav. è anche una norma processuale, destinata a disciplinare il regime probatorio di ammissibilità delle rilevazioni estrapolate dal datore di lavoro grazie ai mezzi di controllo a distanza.

(13) Cass. 3 aprile 2002, n. 4746, *RGL*, 2002, 642 e *MGL*, 2002, 644, nt. Bertocchi.; Cass. 17 luglio 2007, n. 15892, in *RGL*, 2008, 358 e in *RIDL*, 2008, 714, nt. Vallauri; Cass. 23 febbraio 2010, n. 4375, in *RIDL*, 2010, II, 564; Cass. 23 febbraio 2012, n. 2722, *FI*, 2012, I, 1421; Cass. 1 ottobre 2012, n. 16622, *FI*, 2012, I, 3328. Cass. 27 maggio 2015, n. 10955 *FI*, 2015, I, 2316.

(14) P. Lambertucci, *cit.*.

La fattispecie del controllo a distanza realizzato mediante Social network costituisce una testimonianza calzante della sovrapposizione tra condotte illecite ed inadempienti del prestatore di lavoro (15).

Si pensi al caso di un lavoratore che si distragga per molte ore su Facebook in orario di lavoro, postando commenti poco ortodossi sulla clientela, sui colleghi o sul proprio datore di lavoro (16). La distrazione, cioè la sottrazione di tempo all'attività lavorativa, costituisce inadempimento della prestazione principale. Più complessa appare la seconda ipotesi, vale a dire la pubblicazione di un *post* sgradito al datore di lavoro: tale condotta potrebbe costituire un illecito extralavorativo (integrando gli estremi della diffamazione a mezzo stampa) e inadempimento dell'obbligo di diligenza e fedeltà.

L'utilizzo del Social come strumento di controllo a distanza, a scopo difensivo del patrimonio aziendale, peraltro, è stato avallato dalla Suprema Corte, la quale ha stabilito che un controllo di tal fatta, anche se

(15) La spiegazione di questo fenomeno è data dalla progressiva dilatazione degli obblighi di natura accessoria che nascono dal contratto di lavoro, compiuta dalla giurisprudenza. L'effetto di una simile interpretazione si avverte nella trasformazione di illeciti del prestatore di lavoro, astrattamente sussumibili nell'art. 2043 c.c., in fatti di inadempimento contrattuale. Per esemplificare, si pensi alla dilatazione del contenuto dell'obbligo di fedeltà di cui all'art. 2105 c.c.. La giurisprudenza a partire dal *leading case* Cass. 25 febbraio 1986, n. 1173, *FI*,1986, I, 1877 ha accolto una nozione estesa degli obblighi di cui all'art. 2105 c.c., ricomprendendovi anche comportamenti ulteriori che «contrastino con le finalità e gli interessi dell'impresa». Questa estensione dell'obbligo legale viene argomentata facendo leva su concetti eterogenei come la fiducia, la lealtà, la correttezza e la buona fede nell'esecuzione del contratto Da ultimo v. Cass. 9 marzo 2016, n. 4633, in *Il giuslavorista*, 14 marzo 2016, secondo cui il «lavoratore è assoggettato non solo all'obbligo di rendere la prestazione, bensì anche all'obbligazione accessoria di tenere un comportamento extralavorativo che sia tale da non ledere né gli interessi morali e patrimoniali del datore di lavoro né la fiducia che in diversa misura e in diversa forma, lega le parti del rapporto di durata».

(16) L'ipotesi non è fantascientifica, basta dare uno sguardo alle vicende riportate sui quotidiani, che riguardano casi che molto spesso non giungono a sentenza.
Milano, 21 maggio 2009: insoddisfatta della propria condizione lavorativa una dipendente crea un gruppo Facebook così denominato "Noi poveri sfigati che lavoriamo in Danielli"; l'azienda la "convince" a firmare una risoluzione consensuale del contratto di lavoro. Roma, febbraio 2011: il *Sole 24 ore* riporta un caso in Italia di licenziamento via Facebook: un dipendente della Cassa nazionale di previdenza dei commercialisti viene licenziato per aver postato un commento irrispettoso dei propri capi. Empoli, maggio 2014: un'azienda mette in cassa integrazione i propri dipendenti, racconta *Il Tirreno*, i quali commentano acidamente l'accaduto su Facebook. Due di questi vengono "beccati" e licenziati, perché il datore di lavoro "si sentiva minacciato". Ivrea, giugno 2014: il linguaggio irrispettoso e gravemente offensivo di un lavoratore che ha definito "MILF" colleghe e superiori legittima il licenziamento per giusta causa, cfr. Trib. Ivrea, ordinanza 28 gennaio 2015, Dott. Fadda.

occulto, è legittimo in quanto non viola i principi di buona fede e correttezza nell'esecuzione del contratto.

Tuttavia, alla luce del carattere totalizzante del controllo sulla persona permesso dai Social network, si dubita, per una serie di ragioni, della bontà dell'affermazione della Corte. Innanzitutto, l'*escamotage* rappresentato dalla creazione di un profilo *fake* costituisce una indebita intrusione nella sfera giuridica di riservatezza e privacy del lavoratore, protetta non solo dalle norme statutarie ma anche da quelle che disciplinano la materia della privacy. In secondo luogo, tale condotta pare integrare una violazione dei principi di buona fede e correttezza nell'esecuzione del contratto, soprattutto quando il titolare del profilo abbia deciso consapevolmente di utilizzare impostazioni di privacy del profilo tali da restringere la cerchia delle persone che possono accedervi.

Ma, soprattutto, un controllo del genere rappresenta una sorveglianza pura ed esclusiva sull'adempimento della prestazione, nella misura in cui, sotto l'egida dell'esigenza di tutela del patrimonio aziendale, la Cassazione cela la vera sostanza del controllo, vale a dire la verifica del comportamento non diligente di un lavoratore che abbandona gli strumenti di lavoro per socializzare su Facebook.

3. Il nuovo art. 4 St. lav.: come si cambia per non morire

Uno dei decreti attuativi della complessiva Riforma che ha interessato gli istituiti cardine del diritto del lavoro ci ha consegnato un nuovo art. 4. In particolare l'art. 23 d.lgs. 151/2015 ha integralmente sostituito il testo della norma in discussione e dell'art. 171 del Codice della Privacy.

Senza soffermarsi in questa sede su tutti i cambiamenti che hanno riguardato il potere di controllo a distanza giova evidenziarne almeno tre, e cioè quelli che sembrano più rilevanti nell'ipotesi in cui lo strumento di controllo utilizzato dal datore di lavoro sia un Social network.

Una notazione di carattere generale sulla struttura della norma: il legislatore del 2015 ha deciso di attribuire valore giuridico al doppio *step* che l'impresa deve compiere per giovarsi in giudizio delle informazioni raccolte. Disciplina, infatti, in commi separati la fase di installazione delle apparecchiature e quella di utilizzazione dei dati raccolti grazie a queste. Quanto alla installazione, la disciplina diverge a seconda che lo strumento, nel nostro caso il Social, sia uno strumento di controllo o di lavoro. Quanto, invece, all'utilizzo delle informazioni che riguardano il lavoratore, esso è consentito anche a fini disciplinari, a prescindere dal tipo di strumento utilizzato dal datore di lavoro, ma a condizione che la sorveglianza venga effettuata con determinate modalità.

Partendo subito dal punto più spinoso della questione, il comma terzo della norma prevede che, indipendentemente dal tipo di

apparecchio tecnologico installato, gli esiti delle rilevazioni effettuate a distanza sono utilizzabili a tutti i fini connessi al rapporto contrattuale di lavoro, a condizione che il lavoratore risulti adeguatamente informato delle modalità di effettuazione dei controlli e che risulti rispettato il Codice della Privacy. La norma quindi, oggi, consente al datore di lavoro di controllare a distanza il corretto o scorretto svolgimento della prestazione di lavoro (anche sotto il profilo del rendimento del singolo lavoratore); e ciò si desume dalla circostanza che il legislatore permette (17) l'utilizzo dei dati provenienti dal controllo «a tutti i fini» contrattuali in sede di procedimento disciplinare e di processo giudiziale.

Vale la pena fin da subito notare, tuttavia, che questo utilizzo è comunque subordinato al rispetto di alcuni principi scolpiti nel Codice della Privacy e nei provvedimenti dell'Autorità Garante (18), che attengono alle modalità con cui i controlli a distanza dovranno essere effettuati. Principi che sin d'ora si possono riassumere in tre linee direttrici:

- trasparenza e informazione (consapevolezza del controllato);
- prevenzione (obbligo di adottare misure preventive volte a reprimere comportamenti illeciti e abusivi dei dipendenti, degradando il controllo di tipo successivo, cioè sull'illecito già consumato, ad *extrema ratio*);
- proporzionalità (che attiene alle modalità del controllo, che non deve mai essere svolto costantemente in modo indiscriminato e senza soluzione di continuità).

Ma le novità non si esauriscono qui. Nei primi due commi dell'art. 4 St. lav., infatti, il legislatore si preoccupa di disciplinare l'installazione degli strumenti che hanno potenzialità di controllo a distanza «anche dell'attività lavorativa».

Ritaglia, infatti, due fattispecie differenti: gli strumenti di mero controllo e gli strumenti di lavoro, cui corrispondono due discipline differenti in punto d'installazione.

Ed infatti, per installare gli strumenti di puro controllo sono previsti due ordini di limiti: uno di carattere sostanziale e uno di natura procedimentale. Con la stessa tecnica utilizzata dal legislatore del 1970 si prevede, quindi, che gli strumenti che consentono di controllare, a

(17) Lo permette ma non lo impone inderogabilmente. Pertanto è ben possibile che gli accordi sindacali (siglati oggi anche dalla RSU) e i provvedimenti autorizzativi della DTL contengano espressamente il divieto di utilizzo delle rilevazioni a fini disciplinari, come accadeva in passato.

(18) Assumono particolare rilievo nella materia che ci occupa le Linee guida del Garante per l'utilizzo di *internet* e della posta elettronica emanate con Delibera del Garante, 1° marzo 2007, n. 13, G.U. 10 marzo 2007. Per un commento P. Tullini, *Comunicazione elettronica, potere di controllo e tutela del lavoratore,* in *RIDL*, 2009, I, 485; E. Tucci, *Garante per la protezione dei dati personali*, in *FI*, 2007, III, 214.

distanza, anche l'attività lavorativa possano essere installati per far fronte a legittime ragioni dell'impresa, di tipo organizzativo, produttivo, di sicurezza del lavoro e, dopo il 2015, anche di difesa del patrimonio aziendale.

Quanto a quest'ultimo aspetto, è evidente l'intenzione del legislatore di sottoporre la categoria dei controlli difensivi alle garanzie procedurali previste dal nuovo comma 1 dell'art. 4 St. lav., con la finalità di inibire controlli di tipo occulto su comportamenti scorretti dei lavoratori, anche quando ciò sia reso necessario da legittime esigenze di difesa dei beni aziendali materiali e immateriali. Con l'ulteriore effetto di riconoscere che il controllo difensivo si concreta sempre in una sorveglianza indiretta sull'adempimento della prestazione.

Mentre, per quanto attiene al limite procedurale, il datore di lavoro per installare lo strumento di controllo deve procedere a siglare un accordo sindacale (anche con la RSU, ove costituita) o, in difetto di accordo, fare istanza alla DTL (che a breve confluirà nel nuovo Ispettorato Nazionale del Lavoro istituito con d.lgs. 149/2015) per ottenere un'autorizzazione amministrativa (19).

Dalla presenza di causali tipiche e tassative, anche se previste solo per l'installazione di strumenti di controllo, si desume anche nel vigore della norma novellata il divieto di controllo esclusivo dell'attività lavorativa. Per tale dovendosi intendere quella sorveglianza esclusivamente rivolta al controllo sull'esatto o inesatto adempimento del debito lavorativo, non giustificato *a priori* dalla sussistenza di altre finalità ed esigenze aziendali (20).

Dal quadro di garanzie legali sopra tracciato, sono esclusi gli strumenti di lavoro, ovvero quegli strumenti che servono al lavoratore a rendere la prestazione. Il legislatore si affida ad una tecnica descrittiva della fattispecie che fa leva sulla funzione "lavorativa" dello strumento. Senza dire nulla, tuttavia, sulle funzioni di sorveglianza, ad esso

(19) Nella norma è prevista una semplificazione per le imprese con unità produttive dislocate sul territorio nazionale: queste hanno la possibilità di scegliere se stipulare l'accordo sindacale in azienda o a livello nazionale con un'associazione comparativamente rappresentativa ovvero, in difetto di accordo, fare istanza anche al Ministero del Lavoro, ottenendo così una sola volta un accordo/provvedimento valido per tutte le unità produttive.

(20) Sarebbe, infatti, un assurdo logico sostenere che se il datore voglia controllare a distanza *esclusivamente* l'attività lavorativa lo possa fare senza soggiacere a vincoli preventivi e, invece, richiedere l'espletamento della negoziazione sindacale/amministrativa che confermi la presenza di esigenze causali tipiche quando l'imprenditore controlli *anche, ma non solo* la prestazione. L'eliminazione del comma 1 del vecchio articolo 4 St. lav. s'inserirebbe, infatti, in un processo di *maquillage* normativo rivolto a superare la scivolosa distinzione tra controlli intenzionali e preterintenzionali. Cfr. R. Del Punta, *La nuova disciplina dei controlli a distanza sul lavoro (art. 23, d.lgs. 151/2015),* in corso di pubblicazione.

incorporate perché "native" dello strumento, le quali possono "anche riguardare l'attività lavorativa" (21).

Il Social network, data la sua eclettica polivalenza, rappresenta un paradigma perfetto di come la funzione di lavoro e la funzione di controllo possano condensarsi e aggrovigliarsi in un medesimo programma informatico (22).

Ed allora si deve desumere che il legislatore del 2015 abbia non solo voluto semplificare il momento della installazione o meglio consegna di questi strumenti tecnologici, ma anche e soprattutto abbia inteso valorizzare (per non dire "affidare tutto" alla) la consapevolezza individuale del lavoratore che quotidianamente si serve di quello strumento e, quindi, sa di potere essere controllato. Così giungendo a considerare fungibili, nell'era tecnologica, il consenso collettivo e quello individuale.

4. Il nuovo art. 4 e i Social network. Quando il Social è strumento di lavoro.

Nel paragrafo precedente è stato messo in luce che il Social possiede una versatilità tale da essere utilizzato dal dipendente anche per fini lavorativi.

Può infatti accadere che il lavoratore utilizzi la piattaforma sociale per lavorare, e in tal caso il Social avrà la funzione di strumento di lavoro. Ad esempio, è molto frequente che il lavoratore si occupi del cosiddetto *Social media marketing*, curando campagne pubblicitarie e promozionali aziendali, oppure gestendo il servizio clienti e consumatori grazie all'utilizzo di un profilo. In tal caso, l'assegnazione delle credenziali (nome utente e password) potranno certamente essere consegnate al

(21) Vero è che il Comunicato del Ministero del 18 giugno 2015 ha cercato di neutralizzare e sterilizzare la (allora emananda) disposizione. Il ministero aveva proposto, come noto, un'interpretazione restrittiva del concetto di strumento di lavoro, il quale sarebbe tale solo a seguito della "purificazione" di eventuali funzioni di controllo aggiunte sul *device*. Queste ultime andrebbero assoggettate ai vincoli causali e alle regole procedurali dell'art. 4 comma 1 nuovo testo. Sennonché, questa operazione ermeneutica risulta inutile e irrealistica quando la funzione di controllo sia connaturata *ab origine* allo strumento di lavoro e non sia frutto di una modifica (come banalmente avviene quando il lavoratore utilizzi la mail aziendale, che è al contempo strumento di lavoro che costantemente permette il monitoraggio di mittente destinatario e contenuto dei messaggi).

(22) M. Degeorges, *Tweeter au travail est-il passible de licenciement?*, in *www.Les Echos.fr,* 6 marzo 2016 (http://m.lesechos.fr/redirect_article.php?id=021743014033#, ultimo accesso : 19 marzo 2016), riguardante il recentissimo caso di un lavoratore francese che twittava durante l'orario di lavoro dallo *smartphone* aziendale. Il giudice, calcolatrice alla mano, ha stabilito però che il licenziamento (irrogato per colpa grave) era illegittimo in quanto 4 *tweet* al giorno sono "tollerabili" per il datore di lavoro visto che il lavoratore perde circa un minuto per eseguirne uno.

dipendente senza esperire alcuna formalità sostanziale e procedurale. Potrebbe addirittura accadere che l'azienda conosca le password per accedere a quel profilo, che rappresenta evidentemente un mezzo di produzione smaterializzato. Né è necessario che il lavoratore utilizzi il computer aziendale poiché, come noto, una volta che il profilo online sia stato creato vi si può accedere da qualsiasi dispositivo e da qualsiasi luogo.

La consegna dello strumento di lavoro senza vincoli risponde quindi ad esigenze di semplificazione che fanno capo all'interesse dell'impresa e del datore di lavoro. Il problema, però, che si pone riguarda la possibile patologia dell'utilizzo di uno strumento che permette un controllo totalizzante. Il lavoratore, infatti, potrebbe essere licenziato nel caso in cui il datore di lavoro constati un inadempimento contrattuale. Ciò può verificarsi nel caso in cui il lavoratore utilizzi il profilo aziendale per svolgere attività estranee rispetto a quelle per il quale gli è stato concesso (ad es. *chattare* con amici e conoscenti); oppure nell'ipotesi in cui il dipendente manifesti pensieri e opinioni che non risultino in linea con le strategie e le politiche aziendali (23). Ebbene, certamente la norma, ed in particolare il combinato disposto dei commi 2 e 3, autorizza il datore di lavoro ad acquisire questi dati e a utilizzarli come prove dell'inadempimento contrattuale.

Ciò deve tuttavia avvenire nel rispetto di taluni limiti. A seguito della riforma del 2015 il potere di controllo datoriale è esercitato legittimamente se rispetta le disposizioni contenute nel Codice della Privacy e, quindi, anche i provvedimenti del Garante.

Il legislatore è consapevole che le informazioni estrapolate dagli strumenti tecnologici danno vita ad un «trattamento di dati personali» che come tale deve rispondere ai principi sopra richiamati di trasparenza, proporzione e prevenzione.

Di conseguenza, il lavoratore che utilizzi l'*account* per accedere al Social network a fini lavorativi deve essere reso edotto, attraverso apposita informativa, della circostanza che, quando utilizza quel profilo, potrà essere sorvegliato a distanza dal datore di lavoro. Dovrà inoltre sapere preventivamente cosa può fare attraverso quel profilo e cosa no. Ad esempio sarà bene che l'informativa chiarisca se può aggiungere amici, che grado di pubblicità potrà avere quel profilo, se può inserire foto o video riguardanti i locali aziendali etc.

L'informazione e la trasparenza non esauriscono il quadro delle tutele, perché il principio di proporzione si traduce nel divieto assoluto di «controlli prolungati continui e indiscriminati», che sono da considerarsi illeciti. Ciò significa che il datore di lavoro non potrà, certamente,

(23) Vedi *supra,* nota 15, per la qualificazione della manifestazione di opinioni come inadempimento contrattuale.

monitorare in modo costante l'attività del lavoratore sul Social, in ogni istante e in ogni momento in cui è *loggato*.

Inoltre, in omaggio al principio di prevenzione, caro anche al legislatore comunitario, il controllo a distanza di tipo successivo, cioè effettuato sul singolo lavoratore, deve costituire una *extrema ratio* (24).

Quando queste regole siano violate i dati acquisiti a seguito di controllo sulle pagine del Social saranno inutilizzabili in un eventuale procedimento disciplinare e nel successivo giudizio.

5. *Segue.* Quando il Social è strumento di controllo

I principi di trasparenza, proporzione e prevenzione che conformano le modalità di esercizio del potere di controllo a distanza al fine di rendere i dati acquisiti utilizzabili in giudizio, dovranno essere rispettati anche quando, e si tratta della maggior parte dei casi, il Social network non rappresenti un "attrezzo di lavoro".

Ed infatti, può accadere che il datore (o un altro soggetto incaricato) abbia interesse ad accedere al profilo personale del singolo lavoratore, ben sapendo che la consultazione di questo può disvelare una infinità d'informazioni, sia sull'esecuzione (o meno) dell'attività lavorativa che sulla commissione di comportamenti illeciti di svariata natura, profili, come già detto, inscindibilmente connessi e rilevanti ai fini della valutazione datoriale dell'attitudine professionale e della capacità lavorativa del dipendente (25).

Ci insegna il diritto vivente (26) che questo interesse può sorgere non solo perché il datore di lavoro è curioso e ficcanaso, ma anche quando quest'ultimo, insospettito dalla rilevazione di anomalie nel funzionamento della rete *internet* aziendale, senta l'esigenza di verificare quanto tempo i propri dipendenti trascorrano sui Social network in orario di lavoro.

---

(24) L'esercizio del potere di controllo a distanza (di tipo successivo) sul singolo lavoratore deve essere una scelta obbligata a seguito del fallimento di altre modalità di sorveglianza che non coinvolgano dati del singolo lavoratore. Ed infatti il datore deve analizzare dapprima i dati aggregati (quali ad esempio la fascia di consumo o il livello di spesa di una utenza) che garantiscono l'anonimato del singolo e, solo successivamente al riscontro di continue anomalie e irregolarità nell'utilizzo della strumentazione informatica, e comunque previo «avviso generalizzato», garantirgli la possibilità di svolgere indagini individuali sul singolo.

(25) La casistica d'oltreoceano consultabile sul sito *www.firedforfacebook.com* ci consegna una svariata gamma di casi. Ma anche le corti italiane si sono occupate più volte della problematica in questione, cfr. ad es. Trib. Milano, ordinanza, 1 agosto 2014, in *RIDL*, 2014, 1027 con nota di F. Iaquinta, A. Ingrao, *Il datore di lavoro, cit.* Ma vedi anche Cass. 27 maggio 2015, n. 10955, *cit.*

(26) Esperienza raccontata da un direttore del personale al Convegno "*Jobs Act e strumenti di controllo in azienda - L'evoluzione della normativa e delle possibilità per le aziende*" organizzato da Axerta Investigazioni in data 4 febbraio 2016.

Oppure nel caso, apparentemente più complesso, in cui l'imprenditore venga a conoscenza (perché magari avvisato da altri soggetti) della presenza di *post,* foto o video e persino di gruppi (creati direttamente dal singolo dipendente o a cui egli abbia aderito) che risultano sconvenienti per l'immagine del datore di lavoro, *rectius* per il patrimonio aziendale inteso in senso immateriale.

L'ulteriore profilo di complessità deriva dal fatto che l'esercizio del potere di controllo datoriale deve confrontarsi con le impostazioni di privacy del profilo prescelte dal lavoratore. L'utente virtuale, infatti, può stabilire e decidere quale grado di pubblicità attribuire al proprio profilo. Quando il profilo del dipendente sia accessibile solo a "conoscenti" e non sia quindi indiscriminatamente visitabile da chiunque, qualsiasi contenuto pubblicato sulla pagina personale è da considerare riservato. Perché quel filtro per l'accesso adottato costituisce una scelta consapevole di esercitare uno *ius escludendi alios* rispetto alle proprie informazioni personali. La comunicazione non si svolge in un luogo aperto a tutti, ma è riservato solo ai soggetti specificamente autorizzati dal titolare del dato (27). Invece, quando il profilo sia "pubblico" o comunque "visibile agli amici degli amici" (28), *postare* sul Social equivale a renderlo noto alla collettività in un «luogo aperto al pubblico»; di conseguenza il dato è in potenza attingibile da chiunque e quindi anche dal datore di lavoro.

Il nuovo art. 4 St. lav., come è già stato messo in evidenza, ha trasformato il controllo a distanza finalizzato ad accertare comportamenti illeciti ed inadempienti in controllo indiretto sulla prestazione lavorativa. Con la finalità ultima di assoggettare anche questa ipotesi normativa alle garanzie di carattere sostanziale e procedurale già previste dal previgente testo della norma e, al contempo, sottrarla all'imprevedibile ed oscillante giurisprudenza che dominava la materia.

Si può concludere che la posizione del datore di lavoro sia certamente aggravata rispetto al passato. Ed infatti, oggi, quando il datore di lavoro voglia, ad esempio, servirsi di strumenti come il Social network per controllare eventuali condotte illecite e pregiudizievoli del patrimonio aziendale, dovrà sedersi al tavolo di trattativa sindacale e

(27) Di contrario avviso Trib. Bergamo, ord. 24 dicembre 2015, in *il giuslavorista,* 11 gennaio 2016, con nota redazionale *Immagini sconvenienti su facebook: la vita virtuale influisce sul rapporto di lavoro,* nella quale si legge «postare immagini su Facebook equivale, infatti, nella buona sostanza ad inviarle alle persone del proprio circolo di amicizie. La facilità di accesso alle caselle dei colleghi e degli amici, quando anche non sia stata chiesta o concessa una preventiva amicizia, è oramai un fatto notorio».

(28) Anche in quest'ultimo caso il profilo sarebbe visibile ad una cerchia indeterminata di persone. Cfr. Relazione del Garante Privacy per il 2010, *cit.*, 112.

dimostrare che lo svolgimento d'indagini sui profili dei dipendenti si rende necessario ad es. per tutelare i beni immateriali dell'impresa.

Ne deriva che quando il comportamento inadempiente del lavoratore (abuso del *wifi* aziendale per accedere ai Social o distrazione del tempo di lavoro per finalità estranee all'adempimento delle mansioni) sia dovuto all'utilizzo del Social network*,* il datore di lavoro potrà giovarsi delle funzioni di controllo proprie del sistema digitale (geolocalizzazione, memorizzazione dell'orario dei *post*, visibilità pubblica dei contenuti di quest'ultimi) solo quando queste ultime siano state autorizzate da un accordo sindacale (o da un provvedimento della DTL) che accerti l'esigenza aziendale di tutelare il patrimonio aziendale e a condizione che il lavoratore sia informato di questa modalità di controllo a distanza.

Bibliografia

Bellavista A., *Il controllo sui lavoratori*, Giappichelli Editore, 1995;

Degeorges M., *Tweeter au travail est-il passible de licenciement?*, in *www.Les Echos.fr*, 6 marzo 2016;

Liso F., *Computer e controllo dei lavoratori*, *DLRI.,* 1986, 366 ss., 369;

Del Punta R., *La nuova disciplina dei controlli a distanza sul lavoro (art. 23, d.lgs. 151/2015),* in corso di pubblicazione;

Garilli A., *Tutela della persona e tutela della sfera privata nel rapporto di lavoro*, *RCDP*, 1992, II, 321;

Iaquinta F., Ingrao A., *La privacy e i dati sensibili del lavoratore legati all'utilizzo di social networks. Quando prevenire è meglio che curare*, *DRI*, 2014, 1027;

Lambertucci P., *Potere di controllo del datore di lavoro e tutela della riservatezza del lavoratore: i controlli a "distanza" tra attualità della disciplina statutaria, promozione della contrattazione di prossimità e legge delega del 2014 (c.d. Jobs act), CSDLE, It.,* n. 255/2015;

Mini F., *Social Media. Introduction*, in R. Ford, J. Wiederman (edited by), *Internet Case Study Book*, Taschen, 2010, 232;

Romagnoli U., *Sub art. 8*, in G. Ghezzi, F. Mancini, L. Montuschi, U. Romagnoli, *Statuto dei diritti dei lavoratori*, Zanichelli, 1979;

Tucci E., *Garante per la protezione dei dati personali*, in *FI*, 2007, III, 214;

Tullini P., *Videosorveglianza a scopi difensivi e utilizzo delle prove di reato commesso dal dipendente*, *RIDL*, 2011, II, 89;

Tullini P., *Comunicazione elettronica, potere di controllo e tutela del lavoratore,* in *RIDL*, 2009, I, 485.