RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318
Fascicolo 1-2019
DOI: 10.32091/RIID0001

La rilevanza giuslavoristica dei social network, tra diritti dei lavoratori e prerogative datoriali di controllo

Elio Fameli

L'introduzione del computer e l'uso dei social network hanno comportato una vera e propria rivoluzione nel campo delle relazioni sociali e, in particolare, nei rapporti di lavoro. Ovviamente, i profili coinvolti sono numerosi, implicando il sorgere di nuove professionalità e la trasformazione del lavoro subordinato. In tale contesto è urgente prendere coscienza del fatto che l'irrompere delle nuove tecnologie nel mondo del lavoro ha reso possibile la realizzazione e l'impiego di nuove, potenti e insidiose forme di controllo dell'attività dei lavoratori. L'art. 23 del d.lgs. 14 settembre 2015, n. 151, emanato dal Governo in ottemperanza alla legge delega 10 dicembre 2014, n. 183, ponendosi a conclusione d'un lungo e tormentato percorso, ha interamente riscritto l'art. 4 dello Statuto dei lavoratori, ridefinendo i confini del potere datoriale di controllo del lavoratore, anche in relazione all'utilizzo degli strumenti tecnologici attualmente disponibili. Nel contributo, partendo dall'analisi dell'elaborazione giurisprudenziale e degli orientamenti dottrinali in materia di social network e di controlli a distanza sull'attività dei lavoratori, si evidenziano le principali innovazioni introdotte nel passaggio dalla vecchia alla nuova formulazione della norma statutaria, avendo riguardo anche ai connessi problemi di tutela della privacy del lavoratore.

Uso dei social network da parte dei lavoratori – Controlli da parte del datore di lavoro – Tutela della riservatezza dei lavoratori

1. Introduzione: social media e social network nel mondo del lavoro

L'introduzione del computer come indispensabile strumento di lavoro, unitamente alla molteplicità e varietà dei suoi possibili impieghi, ha modificato radicalmente non solo il modo stesso di produrre beni e servizi, ma anche il contesto sociale nel suo complesso. In particolare, i c.d. social (più propriamente, social media) rappresentano un cambiamento fondamentale nel modo di apprendere, acquisire e condividere informazioni e contenuti. La fusione, che in essi

L'A., dirigente di ricerca del CNR in quiescenza, è associato alle ricerche dell'Istituto di Informatica Giuridica e Sistemi Giudiziari (IGSG) del CNR.

si verifica, tra Sociologia e Tecnologia trasforma il "monologo" (da uno a molti) in "dialogo" (da molti a molti), con l'ulteriore effetto di produrre una sorta di democratizzazione dell'informazione in un contesto assolutamente innovativo, in cui le persone si trasformano da meri "fruitori" in "editori" di contenuti.

I "Media Sociali", in questo senso definiti anche UGC - *User-Generated Content* o CGC - *Consumer-Generated Content*, sono divenuti rapidamente molto popolari proprio perché offrono la possibilità di utilizzare la Rete per stabilire e coltivare relazioni di tipo sia personale che lavorativo. È chiaro che si tratta di un fenomeno molto complesso – e, per alcuni versi, anche sfuggente – che ha però la sua principale chiave interpretativa nella configurazione di nuove forme generalizzate di collaborazione e co-creazione di massa dei contenuti informativi. In particolare, sotto il profilo della rivoluzione in atto nel mondo della produzione e distribuzione di beni e servizi, l'utilizzo dei social media da parte di aziende, organizzazioni e consumatori, mediante l'impiego di strutture e tecnologie dedicate, si ritiene che caratterizzi una nuova forma di sistema economico, basata appunto sulla possibilità di creare valore mediante la collaborazione di massa e le piattaforme partecipative[1].

Le diverse configurazioni che i social media possono assumere sono riconducibili ad almeno una decina di categorie, che vanno dai *social network service* ai network di tipo aziendale e professionale, dai *forum Internet* ai *photo* e *video sharing*, dai blog e microblog ai *social gaming* e ai *virtual world*. In particolare, i *social network service*, comunemente chiamati social network, si configurano come servizi Internet, destinati alla gestione di rapporti sociali, che consentono la comunicazione e la condivisione di contenuti testuali e multimediali. Alcuni tra i social network più importanti e diffusi, con centinaia di milioni di utenti iscritti in tutto il mondo, presentano funzionalità molteplici e complesse, tra le quali – a volte – possono presentarsi in maniera nettamente distinta i servizi destinati a soddisfare interessi esclusivamente privati e quelli con finalità di tipo commerciale[2]. È divenuto così estremamente semplice, nella Rete, condividere immagini (foto, video), scambiare messaggi (anche in tempo reale, come avviene nelle on line chat), effettuare chiamate vocali, pubblicare scritti e articoli, inserire annunci pubblicitari, esprimere commenti, condivisioni e apprezzamenti[3], effettuare ricerche sui contenuti dei profili degli utenti e degli amici a questi collegati.

All'incidenza di questa vera e propria rivoluzione tecnologica sulle relazioni sociali e, in particolare, sui rapporti di lavoro è stata rivolta, nel tempo, l'attenzione di numerosi autorevoli studiosi che, prendendo atto dei profondi e irreversibili cambiamenti in corso nell'organizzazione del lavoro e dei sistemi di produzione, hanno opportunamente riconsiderato l'impianto complessivo della disciplina del rapporto di lavoro e delle relazioni industriali nella struttura dell'impresa. Ovviamente, i profili coinvolti sono numerosi, implicando il sorgere di nuove professionalità, ma anche, più in generale, un diverso inquadramento del lavoro subordinato. Soprattutto, però, per quanto specificamente attiene al tema che qui si affronta, è inevitabile prendere coscienza del fatto che l'irrompere delle nuove tecnologie nel mondo del lavoro ha comportato anche la realizzazione e l'impiego di nuove, potenti e insidiose forme di controllo dell'attività dei lavoratori.

Punto d'arrivo di questo acceso dibattito – in cui spesso si sono trovate contrapposte le posizioni della dottrina, più sensibile alle esigenze garantistiche di tutela del lavoratore in opposizione all'invasività dei controlli tecnologici datoriali, e quelle della giurisprudenza, in generale più aperta alla possibilità d'un riconoscimento della legittimità dei controlli aziendali – è stato l'intervento normativo deciso dal Governo Renzi. Come è noto, infatti, con la l. 10 dicembre 2014, n. 183 il Parlamento ha delegato il Governo ad emanare uno o più decreti legislativi, nel rispetto dei principî e criteri direttivi indicati nel medesimo provvedimento, ma anche in coerenza con la regolazione dell'Unione europea e con le Convenzioni internazionali, al fine di realizzare «una revisione della disciplina dei controlli a distanza sugli impianti e sugli strumenti di lavoro, tenendo conto dell'evoluzione tecnologica e contemperando le esigenze produttive ed organizzative dell'impresa con la tutela della dignità e della riservatezza del lavoratore»[4].

Come sarà precisato nel seguito della trattazione, l'art. 23, d.lgs. 14 settembre 2015, n. 151, emanato dal Governo in ottemperanza alla legge delega, ponendosi a conclusione d'un lungo e tormentato percorso, ha interamente riscritto l'art. 4 dello Statuto dei lavoratori, ridefinendo i confini del potere datoriale di controllo del lavoratore, anche in relazione all'utilizzo degli strumenti tecnologici attualmente disponibili.

2. Il controllo dell'attività dei lavoratori: inquadramento normativo

La rapida evoluzione tecnologica in corso, soprattutto nel campo della comunicazione e della interazione a distanza, ha modificato profondamente lo scenario in cui si era mosso il legislatore del 1970, rendendo necessaria una profonda revisione della normativa allora vigente. Fermo restando l'obiettivo di conciliare,

da un lato, le esigenze del datore di lavoro connesse al legittimo esercizio del potere direttivo e, dall'altro, il diritto del lavoratore al rispetto della propria libertà, dignità e riservatezza, il dibattito in materia di limiti del potere di controllo datoriale sull'attività del lavoratore si è incrementalmente alimentato sulla base di una casistica sempre più estesa e, originariamente, imprevedibile[5].

Il datore di lavoro ha il potere di controllare che il lavoratore, nell'esecuzione della prestazione lavorativa, usi la diligenza dovuta (art. 2104, *Diligenza del prestatore di lavoro*, co. 1 c.c.), osservi le disposizioni impartitegli (art. 2104, co. 2 c.c.) e rispetti gli obblighi di fedeltà sullo stesso gravanti (art. 2105 c.c., *Obbligo di fedeltà*), anche al fine di poter esercitare l'eventuale azione disciplinare nel caso in cui rilevi l'inosservanza di tali obblighi (art. 2106 c.c., *Sanzioni disciplinari*, art. 7 dello Statuto dei lavoratori). Tale potere, tuttavia, non è assoluto, in quanto si pone come limite la necessità che esso sia esercitato in modo tale da non ledere diritti fondamentali del lavoratore, quali sono appunto la sua libertà, dignità e riservatezza.

Per quanto riguarda, poi, le modalità del controllo occorre fare riferimento all'articolo 4 dello Statuto dei lavoratori (l. 20 maggio 1970, n. 300, *Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento*) che, sotto la rubrica *Impianti audiovisivi*, contiene la normativa in materia di "controlli a distanza dell'attività dei lavoratori". Tali norme sono state modificate, a decorrere dal 24 settembre 2015[6], dall'art. 23, d.lgs. 14 settembre 2015, n. 151 (c.d. *Decreto semplificazioni*), promulgato in attuazione della delega conferita al Governo con la legge 10 dicembre 2014, n. 183 (art. 1, co. 7, lett. *f*), nell'ambito dell'ampio intervento di riforma del mercato del lavoro denominato "Jobs Act". Successivamente, a decorrere dall'8 ottobre 2016[7], le stesse norme sono state aggiornate con le integrazioni apportate dall'art. 5, co. 2, d.lgs. 24 settembre 2016, n. 185[8].

Attualmente, dunque, il testo dell'art. 4 dello Statuto dei lavoratori, significativamente collocato all'interno del Titolo I (*Della libertà e dignità del lavoratore*), nel suo insieme risulta essere quello sostituito alla versione originaria del 1970 dall'art. 23, co. 1, d.lgs. 14 settembre 2015, n. 151; inoltre, dei tre commi di cui l'articolo si compone, il primo è stato successivamente modificato dall'art. 5, co. 2, d.lgs. 24 settembre 2016, n. 185.

3. Le limitazioni al controllo datoriale dell'attività dei lavoratori. Divieto "assoluto" e divieto "flessibile" del controllo a distanza nella formulazione originaria dell'art. 4 dello Statuto dei lavoratori

Per una corretta interpretazione dell'attuale art. 4 dello Statuto occorre prendere in considerazione i forti cambiamenti che, nel giro di breve tempo, hanno radicalmente trasformato l'intero contesto di riferimento e, in particolare, le caratteristiche e le funzionalità degli strumenti concretamente utilizzabili per l'effettuazione del controllo, come anche per la prestazione dell'attività lavorativa.

Come già indicato, tra i poteri del datore di lavoro rientra anche quello di controllare l'esatta esecuzione della prestazione lavorativa dedotta in contratto, verificando se il dipendente usi la prescritta diligenza (art. 2104, co. 1, c.c.) e osservi le disposizioni impartitegli (art. 2104, co. 2, c.c.), anche in ordine all'eventuale esercizio del potere disciplinare (art. 2106 c.c.; art. 7 St. lav.), potere rispetto al quale la possibilità d'effettuare controlli risulta funzionalmente collegata. Restando però ineludibile l'esigenza del contemperamento tra l'esercizio del potere di controllo da parte del datore di lavoro e il rispetto delle libertà fondamentali del lavoratore, cui occorre riconoscere dignità giuridica pari alle contrapposte esigenze datoriali, il legislatore, nello Statuto dei lavoratori, ha disposto precise limitazioni al potere datoriale di controllo, con riferimento all'impiego delle guardie giurate (divieto di controllo da parte delle guardie giurate: art. 2, co. 3, St. lav.), al personale di vigilanza (divieto di controllori ignoti: art. 3 St. lav.), ai controlli a distanza (divieto di controlli a distanza: art. 4 St. lav.), alle visite personali di controllo (i relativi limiti sono indicati nell'art. 6 St. lav.) e alle opinioni personali del lavoratore (divieto di indagini sulle opinioni: art. 8 St. lav.).

All'interno della disciplina dei controlli contenuta nello Statuto dei lavoratori (agli artt. da 2 a 8), in riferimento al tema specifico della presente trattazione rilevano soprattutto le disposizioni di cui all'art. 4 che, nella versione attualmente in vigore, è il risultato della sostituzione operata, insieme all'art. 171 del Codice della privacy, dal d.lgs. 151/2015 (all'art. 23), nell'ambito della complessiva riforma degli istituti cardine del diritto del lavoro operata con il Jobs Act[9].

L'art. 4 dello Statuto dei Lavoratori, nella sua formulazione originaria, vietava espressamente (co. 1) l'utilizzo di impianti audiovisivi e di altre appa-

recchiature che avessero quale finalità determinante ed esclusiva il controllo a distanza dell'attività lavorativa. Il legislatore del 1970, che certamente nel disciplinare la fattispecie del controllo a distanza non poteva prendere in considerazione anche i social network, al comma 1 del vecchio art. 4, esordiva vietando categoricamente, come principio di carattere generale, «l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori». Dunque, mentre il controllo effettuato "di persona" veniva sottoposto ai limiti di cui agli artt. 2 e 3 dello Statuto dei lavoratori, era invece vietata in ogni caso l'effettuazione, da parte del datore di lavoro, del controllo a distanza sul corretto svolgimento dell'attività lavorativa.

La differenza sostanziale tra controlli "umani" – svolti dall'uomo, necessariamente in presenza del sorvegliato, che è comunque in grado di rendersi conto del controllo in atto – e controlli "tecnologici" – effettuati a distanza, sia in senso spaziale che temporale, grazie all'impiego di strumenti atti ad acquisire rapidamente grandi quantità d'informazioni, memorizzandole per poi renderle disponibili anche dopo molto tempo – aveva indotto il legislatore ad assumere posizioni nettamente distinte nelle due ipotesi, ammettendo il controllo "di persona", sia pur sottoposto ai limiti di cui agli artt. 2 e 3 dello Statuto dei lavoratori, nella prima ipotesi, e fissando un divieto di carattere generale nella seconda.

Il divieto posto al controllo a distanza dell'attività lavorativa era sanzionato penalmente nell'art. 38 dello Statuto e si configurava, quindi, come assoluto e inderogabile per quanto attenesse sia all'installazione che all'uso di impianti audiovisivi e di altre apparecchiature destinate esclusivamente al controllo dell'attività dei lavoratori.

Il secondo comma dell'art. 4, invece, regolando la possibilità, per il datore di lavoro, di installare «gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori», veniva teoricamente a configurare la legittimità d'una categoria di strumenti (impianti e apparecchiature) il cui impiego fosse reso necessario dalle esigenze organizzative e produttive o dalla sicurezza del lavoro, e tutto ciò anche in presenza di una esplicita previsione normativa della loro utilizzabilità per il controllo a distanza dell'attività dei lavoratori, al di là delle intenzioni del datore di lavoro.

Al divieto "assoluto", previsto nel primo comma dell'art. 4, veniva così ad affiancarsi, nel secondo comma dello stesso articolo, un divieto per così dire "flessibile", in quanto, nella previsione del legislatore, il riconoscimento dell'esistenza di esigenze della organizzazione, della produzione e della sicurezza del lavoro, nei confronti delle quali gli strumenti in questione fossero da considerare strettamente funzionali, consentiva l'installazione di impianti e di apparecchiature dai quali poteva derivare "anche la possibilità di controllo a distanza dell'attività dei lavoratori".

In ogni caso, però, per la legittimità dell'installazione erano necessari, oltre alla finalità di tutela delle suindicate esigenze aziendali, l'accordo con le rappresentanze sindacali o, in mancanza, l'autorizzazione amministrativa da parte del servizio ispettivo della Direzione Territoriale del lavoro competente per territorio (Ispettorato Territoriale del lavoro). L'effettiva sussistenza delle esigenze imprenditoriali suindicate, costituendo oggetto di preventiva verifica in ordine al conseguimento dell'accordo o dell'autorizzazione, da un lato si configurava come base imprescindibile per legittimare l'installazione di impianti e apparecchiature di sorveglianza, dall'altro valeva a escludere la utilizzabilità delle informazioni acquisite mediante tali strumenti in ordine a finalità diverse da quelle connesse, appunto, con le necessità aziendali in materia di organizzazione, produzione e sicurezza del lavoro.

4. "Controlli preterintenzionali" (o "indiretti"), "controlli difensivi" e "controlli occulti" nella elaborazione giurisprudenziale della Suprema Corte

4.1. I "controlli preterintenzionali" (o "indiretti")

Il divieto "assoluto" del controllo a distanza dell'attività dei lavoratori, già sotto il vigore dell'art. 4 dello Statuto nella sua formulazione originaria, veniva estensivamente interpretato fino a ricomprendere ogni forma di «controllo continuo» o, comunque, «attuabile in qualunque momento», da parte del datore di lavoro, sulla prestazione lavorativa. Pertanto, l'oggetto del divieto veniva inteso nel senso di ricomprendere «qualsiasi forma di controllo a distanza che sottragga al lavoratore, nello svolgimento delle sue mansioni, ogni margine di spazio o di tempo nel quale egli possa essere ragionevolmente certo di non essere osservato, ascoltato o comunque 'seguito' nei suoi movimenti»[10].

Per contro, il divieto "flessibile" di cui al secondo comma dello stesso art. 4 apriva alla possibilità, da parte del datore di lavoro, dei controlli c.d. "preterintenzionali" o "indiretti", cioè di quei controlli che, pur essendo primariamente volti a fini organizzativi o produttivi o alla tutela della sicurezza del lavoro, potessero comunque comportare, come conseguenza indiretta, lo svolgimento d'un controllo sull'attività del

lavoratore, fermi restando il limite "esterno", rappresentato dalla necessità dell'autorizzazione sindacale o amministrativa, e il limite "interno" della conformità alle esigenze tecnico-produttive o di sicurezza individuate in sede autorizzatoria[11].

4.2. I "controlli difensivi"

Alla nozione generale del divieto "flessibile" era venuta successivamente a collegarsi, in forza soprattutto dell'elaborazione giurisprudenziale svolta dalla Suprema Corte, la categoria dei controlli c.d. "difensivi", in quanto controlli messi in atto dal datore di lavoro al fine di accertare condotte illecite del lavoratore[12]. Sul presupposto della necessità di tutelare l'interesse del datore di lavoro a preservare l'integrità del patrimonio aziendale, la giurisprudenza riteneva – sia pure con pronunce di contenuto non sempre univoco – che questa tipologia di controlli fosse sottratta all'ambito d'applicazione dell'art. 4 dello Statuto.

Così, nella sentenza n. 4746 del 3 aprile 2002[13] la Corte di Cassazione aveva escluso che il divieto di utilizzo di apparecchiature per il controllo a distanza dell'attività dei lavoratori, previsto dall'art. 4 dello Statuto, potesse considerarsi operativo anche nel caso in cui i controlli effettuati dal datore di lavoro avessero ad oggetto, direttamente o indirettamente, non la prestazione lavorativa, bensì gli illeciti eventualmente commessi dal dipendente. In un primo momento, dunque, la Suprema Corte aveva ritenuto che i "controlli difensivi" fossero legittimi in ogni caso, a prescindere anche dalla valutazione del loro grado d'invasività.

Le critiche espresse in dottrina[14] e l'evoluzione in senso diverso della prevalente giurisprudenza di merito[15] hanno successivamente indotto i giudici di legittimità ad assumere una più cauta impostazione argomentativa. L'orientamento inizialmente espresso nel senso di sottrarre del tutto al divieto categorico contenuto nel primo comma dell'originario art. 4 dello Statuto forme di controllo datoriale volte ad accertare condotte illecite del lavoratore, venne pertanto a stemperarsi nel tempo, riconoscendo – i giudici della stessa Corte – l'applicabilità dell'art. 4 e dei vincoli procedurali in esso previsti anche nelle ipotesi in cui i controlli diretti ad accertare illeciti del lavoratore avessero comunque ad oggetto comportamenti riguardanti «l'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro e non la tutela di beni estranei al rapporto stesso».

Così, diversamente dalla pronuncia del 2002, con la sentenza n. 15892 del 17 luglio 2007[16] la Cassazione affermò che l'adozione di controlli difensivi non poteva di per sé giustificare un sostanziale annullamento di ogni forma di garanzia della dignità e riservatezza del lavoratore. Al requisito della – non facile – individuazione dell'oggetto del controllo si aggiungeva poi anche la rilevanza delle sue modalità esecutive, ricollegabili all'impiego di «strumenti che presentano quei requisiti strutturali e quelle potenzialità lesive, la cui utilizzazione è subordinata al previo accordo con il sindacato o all'intervento dell'Ispettorato del lavoro». Il raggiungimento dell'accordo sindacale o il conseguimento dell'autorizzazione amministrativa sarebbero stati pertanto necessari a garantire, in queste ipotesi, la conoscenza del controllo da parte dei dipendenti, in ordine alla determinazione, in maniera trasparente, di misure atte a tutelare la loro dignità e riservatezza.

A questo punto importa qui rilevare che questo principio, enucleato dalla Cassazione con riferimento ai controlli difensivi sottoposti comunque alla operatività dei limiti fissati nel secondo comma dell'originario art. 4 dello Statuto, pur basandosi sulla non sempre agevole possibilità di distinguere tra controlli riguardanti l'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro e controlli attinenti alla tutela di beni estranei al rapporto lavorativo, è stato riaffermato in numerose pronunce successive e, con la sentenza n. 4375 del 23 febbraio 2010[17], è stato esteso ai «programmi informatici che consentono il monitoraggio della posta elettronica e degli accessi ad Internet». Anzi, secondo i giudici della Corte, tali programmi sarebbero necessariamente da considerare "apparecchiature di controllo" ai sensi del co. 2, art. 4, in quanto, «in ragione delle loro caratteristiche, consentono al datore di lavoro di controllare a distanza e in via continuativa, durante la prestazione, l'attività lavorativa e se la stessa sia svolta in termini di diligenza e di corretto adempimento».

Prescindendo dalla specifica vicenda da cui tale pronuncia ha preso le mosse e dalle questioni di diritto ad essa sottese, alla sentenza in questione occorre attribuire un'importanza particolare nella misura in cui viene a configurarsi come espressione d'una nuova consapevolezza nell'ambito della giurisprudenza di legittimità: si prende atto, cioè, della diversa – e sempre crescente – pervasività delle forme di controllo datoriale rese possibili dalle nuove tecnologie e si riconosce che gli strumenti atti a consentire forme di controllo a distanza dell'attività dei lavoratori sono sempre più potenti e versatili, per cui il loro impiego permette d'effettuare verifiche analitiche e continue – in tempo reale, ma anche in momenti successivi – di tutto quanto sia stato compiuto o si sia comunque verificato in un dato luogo e in un periodo di tempo determinato.

In linea con il principio ispiratore della sentenza da ultimo citata è, ancora, la pronuncia della Cassazione 1° ottobre 2012, n. 16622[18], con cui i giudici hanno ritenuto illegittimo il comportamento del datore di lavoro che, mediante un apposito software, aveva posto in essere forme di controllo a distanza sull'attività del lavoratore al fine di valutarne la produttività e successivamente deciderne il licenziamento. Nella fattispecie la Corte aveva precisato che i controlli difensivi devono conservare le garanzie procedurali previste dallo Statuto dei lavoratori e «non possono impingere la sfera della prestazione lavorativa dei singoli lavoratori». Pertanto, «qualora interferenze con quest'ultima vi siano, e non siano stati adottati dal datore di lavoro sistemi di filtraggio per non consentire, in ragione della previsione dell'art. 4, comma 1, di risalire all'identità del lavoratore, i relativi dati non possono essere utilizzati per provare l'inadempimento contrattuale del lavoratore medesimo».

Sulla necessità dell'accordo con le rappresentanze sindacali (o, in mancanza, dell'autorizzazione amministrativa da parte dell'Ispettorato del lavoro), anche in presenza di esigenze organizzative e produttive ovvero di tutela del patrimonio aziendale e della sicurezza del lavoro, si è pronunciata la Corte di Cassazione penale con la sentenza n. 22148 dell'8 maggio 2017, relativa al ricorso presentato dalla titolare di un negozio, condannata per la violazione dell'art. 4 dello Statuto dei Lavoratori, in quanto aveva installato, all'interno del luogo di lavoro, un impianto di videoripresa sulla base del mero consenso orale dei lavoratori al trattamento dei propri dati personali, ma senza la previa stipulazione di un accordo con le rappresentanze sindacali e in assenza dell'alternativa autorizzazione da parte dell'Ispettorato del lavoro. Ricostruendo il contesto normativo di riferimento, la Cassazione ha evidenziato come, in tema di divieto di uso di impianti audiovisivi e di altri strumenti da cui discenda anche la possibilità di un controllo a distanza dei lavoratori, sussista continuità di tipo di illecito tra la previgente fattispecie – prevista dagli arrt. 4 e 30, comma 1, dello Statuto dei Lavoratori e dagli artt. 114 e 171 del d.lgs. n. 196 del 2003 – e quella attualmente vigente, parzialmente ridimensionata dall'art. 23 del d.lgs. n. 151 del 2015 (attuativo di una delle deleghe contenute nel c.d. "Jobs Act"), avendo la normativa sopravvenuta mantenuto immutata la disciplina sanzionatoria per cui la violazione del citato articolo 4 è penalmente sanzionata ai sensi dell'art. 38. Pertanto la Suprema Corte ha affermato che, anche in presenza di un consenso validamente espresso da parte dei lavoratori interessati, una condotta del datore di lavoro come quella del caso di specie produce l'oggettiva lesione degli interessi collettivi di cui le rappresentanze sindacali sono portatrici, in quanto esse sono deputate a riscontrare, negli impianti audiovisivi di cui il datore di lavoro intende avvalersi, la loro eventuale idoneità a ledere la dignità dei lavoratori o, al contrario, la loro effettiva rispondenza alle esigenze tecnico-produttive o di sicurezza, disciplinandone, in questa ipotesi, mediante l'accordo collettivo, le modalità e le condizioni d'uso[19].

Per l'opposta ipotesi dell'espletamento di un'attività datoriale di sorveglianza avente ad oggetto comportamenti illeciti del lavoratore che attengano non all'esatto adempimento di obbligazioni discendenti dal rapporto di lavoro, bensì alla tutela di beni estranei al rapporto stesso, conformemente al principio enunciato nella già citata sentenza del 2007, si è formata una non esigua giurisprudenza in cui si è con coerenza affermata l'esclusione dal campo d'applicazione dell'art. 4 dello Statuto. Nel caso preso in considerazione dai giudici della Suprema Corte nella sentenza del 23 febbraio 2012, n. 2722[20], ad esempio, l'attività di controllo che il datore di lavoro aveva posto in essere sulle strutture informatiche aziendali, prescindendo dalla «pura e semplice sorveglianza sulla esecuzione della prestazione lavorativa degli addetti», era invece «diretta ad accertare un comportamento che poneva in pericolo la stessa immagine dell'azienda presso terzi». La Corte ha quindi ritenuto che il datore di lavoro potesse legittimamente esercitare tale forma di controllo avvalendosi degli strumenti derivanti dall'esercizio dei poteri connessi alla sua posizione di supremazia sulla struttura aziendale e in relazione al riconoscimento normativo del diritto datoriale di tutelare il patrimonio aziendale, considerato comprensivo non solo del complesso dei beni dell'impresa, ma anche della sua immagine esterna, così come accreditata presso il pubblico.

Il principio affermato nelle pronuncia sopra richiamata è stato anche di recente ripreso dalla Suprema Corte con l'ordinanza n. 13266 del 28 maggio 2018. In essa si sostiene, infatti, la legittimità di un licenziamento disciplinare adottato dal datore di lavoro a seguito di controlli retrospettivi effettuati sul personal computer in dotazione di un dipendente. Risultando che il lavoratore aveva utilizzato in maniera continuativa il computer aziendale per fini personali ed extralavorativi, la Suprema Corte è tornata sul tema dei controlli difensivi e dell'ambito di operatività dell'art. 4 comma 2, St. Lav. (nella versione antecedente al d. lgs. n. 151/2015) per affermare che "in tema di controllo del lavoratore, le garanzie procedurali poste dalla L. 300/1970, art. 4, comma 2 (accordo sindacale preventivo oppure, in mancanza, autorizzazione dell'Ispettorato del lavoro), trovano

applicazione ai controlli c.d. difensivi, diretti ad accertare comportamenti illeciti dei lavoratori, quando, però, tali comportamenti riguardino l'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro e non, invece, quando attengano alla tutela di beni estranei al rapporto stesso". In conseguenza si è ritenuto che esuli dal campo d'applicazione della norma sopra citata il caso in cui il datore di lavoro abbia posto in essere verifiche volte ad accertare comportamenti del prestatore che si configurino come illeciti e lesivi del patrimonio e dell'immagine dell'azienda[21].

A conclusione di questa breve rassegna giurisprudenziale, tra le pronunce delle Corti di merito è opportuno qui incidentalmente citare la recente ordinanza, n. 57668 del 13 giugno 2018, in cui il Tribunale di Roma ha affrontato il tema della nuova disciplina dei controlli a distanza e della utilizzabilità delle informazioni raccolte dopo la novella apportata all'art. 4, l. n. 300/1970, dall'art. 23, comma 1, d.lgs. n. 151/2015, sostenendo l'attuale inesistenza, in termini assoluti, di un divieto di effettuare controlli a distanza sui lavoratori. Sarebbe pertanto inutile appellarsi a "finalità difensive" per superare un divieto assoluto da considerare come attualmente non più configurabile. Per converso, sulle modalità di esecuzione del controllo, la novella ha posto limiti chiari e rigorosi, la cui osservanza non può più risultare eludibile mediante il ricorso alla figura dei c.d. controlli difensivi. Secondo quanto si afferma nell'ordinanza, il legislatore sembra avere ormai superato la logica per cui il lavoratore non può essere controllato a distanza salvo che non si dimostri che ci si è dovuti difendere da comportamenti illeciti, idonei a ledere il patrimonio e l'immagine dell'azienda. Viene, invece, realizzato normativamente un opportuno contemperamento tra l'interesse al controllo e l'esigenza di protezione della dignità e riservatezza dei lavoratori, per tal via sottratte alle oscillazioni della giurisprudenza in materia: in sintesi, il lavoratore può essere sottoposto a controlli a distanza, ma comunque sempre nel rispetto di precise condizioni[22]. L'importanza di questa recente pronuncia del Tribunale di Roma sembra dunque da ricollegare alla tesi secondo cui sussisterebbe un vero e proprio rapporto di propedeuticità tra il rispetto della normativa posta a tutela dei dati personali e l'utilizzabilità – in relazione a tutti i fini connessi al rapporto di lavoro – delle informazioni raccolte attraverso l'utilizzo di strumenti tecnologici da parte del dipendente.

4.3. I "controlli difensivi occulti"

Una necessaria integrazione sull'orientamento dei giudici di legittimità in materia di "controlli difensivi" messi in atto dal datore di lavoro è quella che riguarda la sottospecie dei c.d. "controlli difensivi occulti", svolti appunto all'insaputa del lavoratore. In questa sede ci si limita a citare solo alcune tra le principali sentenze afferenti alla questione. Da esse può trarsi il principio della "tendenziale ammissibilità" di questa particolare tipologia di controlli, in quanto «diretti all'accertamento di comportamenti illeciti del lavoratore che risultino diversi dal mero inadempimento della prestazione lavorativa, sotto il profilo quantitativo e qualitativo, ma incidano sul patrimonio aziendale, ferma comunque restando la necessaria esplicazione delle attività di accertamento mediante modalità non eccessivamente invasive e rispettose delle garanzie di libertà e dignità dei dipendenti, con le quali l'interesse del datore di lavoro al controllo e alla difesa della organizzazione produttiva aziendale deve contemperarsi e, in ogni caso, sempre secondo i canoni generali della correttezza e buona fede contrattuale».

In questi termini si è espressa la Cassazione in una importante sentenza del 2015[23], in cui si precisa, tra l'altro, che le norme poste dalla l. 300/1970, agli artt. 2 e 3, a tutela della libertà e dignità del lavoratore, delimitano la sfera d'intervento delle persone preposte dal datore di lavoro a difesa dei suoi interessi, con specifiche attribuzioni nell'ambito dell'azienda (guardie giurate e personale di vigilanza, rispettivamente, con poteri di polizia giudiziaria e di controllo della prestazione lavorativa), ma non escludono il potere dell'imprenditore, ai sensi degli artt. 2086 e 2104 c.c., di controllare – direttamente o mediante la propria organizzazione gerarchica o anche attraverso personale esterno (costituito, in ipotesi, da dipendenti di una agenzia investigativa) – l'adempimento delle prestazioni lavorative e quindi di accertare mancanze specifiche dei dipendenti, già commesse o in corso di esecuzione. Questo principio, ad avviso dei giudici della Corte, sarebbe comunque valido, «indipendentemente dalle modalità del controllo, che può avvenire anche occultamente, senza che vi ostino né il principio di correttezza e buona fede nell'esecuzione dei rapporti, né il divieto di cui alla stessa L. n. 300 del 1970, art. 4, riferito esclusivamente all'uso di apparecchiature per il controllo a distanza [...]».

Nella fattispecie presa in esame dai giudici di legittimità il responsabile del personale all'interno della società datrice di lavoro aveva compiuto un accertamento delle conversazioni intrattenute via Internet dal dipendente mediante il suo cellulare. La particolarità del controllo a distanza effettuato consisteva nel fatto che l'accertamento in questione era stato reso possibile attraverso la creazione di un "falso

profilo di donna sulla rete Facebook", profilo con il quale il dipendente ignaro aveva poi "chattato in più occasioni", in orari che la stessa azienda aveva riscontrato concomitanti con quelli di lavoro e da posizione – accertata sempre attraverso Facebook – coincidente con la zona industriale in cui aveva sede lo stabilimento della società.

Pur tenendo fermo il principio per cui l'esigenza del datore di lavoro di evitare condotte illecite da parte dei dipendenti non può assumere portata tale da giustificare un sostanziale annullamento di ogni forma di garanzia della dignità e riservatezza del lavoratore, la Corte ha ritenuto che la fattispecie considerata rispettasse questi limiti e si ponesse «al di fuori del campo di applicazione dell'art. 4 dello Statuto», in quanto il datore di lavoro aveva posto in essere un'attività di controllo avente ad oggetto non l'attività lavorativa in senso proprio e il suo esatto adempimento, bensì l'eventuale perpetrazione di comportamenti illeciti da parte del dipendente, comportamenti poi effettivamente riscontrati. Il controllo difensivo occulto era dunque teso a riscontrare e sanzionare un comportamento idoneo a ledere il patrimonio aziendale sotto il profilo del regolare funzionamento e della sicurezza degli impianti.

Secondo i giudici della Corte, inoltre, neanche la creazione del falso profilo Facebook sarebbe stata, di per sé, configurabile come violazione dei principî di buona fede e correttezza nell'esecuzione del rapporto di lavoro, in quanto attinente «a una mera modalità di accertamento dell'illecito commesso dal lavoratore, non invasiva né induttiva all'infrazione». Altrettanto doveva dirsi, poi, con riguardo alla localizzazione del dipendente, avvenuta in conseguenza dell'accesso a Facebook da cellulare e, quindi, nella presumibile consapevolezza del lavoratore di poter essere localizzato attraverso il sistema di rilevazione satellitare del suo cellulare[24].

Tuttavia, proprio il carattere totalizzante del controllo sulla persona realizzabile mediante i social network ha indotto la dottrina a dubitare della coerenza e correttezza delle affermazioni della Corte rilevandosi, nella creazione di un falso profilo Facebook, una violazione dei principî di buona fede e correttezza nell'esecuzione del contratto, oltre che una indebita intrusione nella sfera giuridica di riservatezza del lavoratore[25].

Infine, la Corte di Cassazione (Sezione Lavoro), con sentenza 10 novembre 2017, n. 26682, ha stabilito che, in tema di controllo dell'attività dei lavoratori, le garanzie procedurali (accordo sindacale o autorizzazione amministrativa) imposte dall'art. 4, co. 2, l. 300/1970 (nella versione originaria antecedente alla formulazione disposta dall'art. 23, d.lgs. 151/2015) per l'installazione di impianti e apparecchiature di controllo richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, dai quali derivi la possibilità di verifica a distanza dell'attività dei lavoratori, trovano applicazione ai controlli c.d. difensivi, diretti ad accertare comportamenti illeciti dei lavoratori, quando, però, tali comportamenti riguardino l'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro e non, invece, la tutela di beni estranei al rapporto stesso. Ne consegue che esula dal campo di applicazione della norma il caso in cui il datore di lavoro abbia posto in essere verifiche dirette ad accertare comportamenti del prestatore illeciti e lesivi del patrimonio aziendale e, quindi, anche dell'immagine presso terzi.

5. Il controllo a distanza dell'attività lavorativa nel passaggio dal vecchio al nuovo art. 4 dello Statuto

5.1. La distinzione tra "installazione" e "impiego" degli strumenti di controllo

In base a una interpretazione ampiamente diffusa – e comunque supportata anche dalle precisazioni definitorie contenute nella giurisprudenza della Cassazione[26] –, la locuzione "controllo a distanza" sarebbe da intendere sia in senso spaziale che temporale. Nel contesto che qui specificamente rileva, è evidente che il controllo tecnologico si svolge a distanza sia di spazio che di tempo in quanto gli strumenti disponibili consentono d'acquisire agevolmente e rapidamente grandi quantità di dati e informazioni, memorizzandole, conservandole e rendendole consultabili in qualunque momento, anche per lunghi periodi.

Per quanto riguarda, invece, l'oggetto del controllo, tanto nella versione originaria che in quella modificata dal legislatore nel 2015, esso è individuato dall'espressione "attività dei lavoratori", riferibile ai comportamenti messi in atto per l'espletamento della prestazione lavorativa, ma anche a quelli non rientranti nel vincolo di subordinazione tecnico-funzionale del lavoratore, in quanto consistenti in «quei gesti e comportamenti di carattere personale di cui è costellata la giornata lavorativa» (c.d. "licenze comportamentali")[27].

Nel passaggio dalla vecchia alla nuova formulazione dell'art. 4 dello Statuto si può osservare che, mentre sono rimaste invariate le espressioni fondamentali di riferimento sopra brevemente illustrate ("controllo a distanza" e "attività dei lavoratori"), nell'attuale primo comma è stata invece introdotta una distinzione terminologica prima assente nel testo normativo. Il legislatore sembra infatti voler considerare auto-

nomamente il momento della "installazione" e quello relativo alla "utilizzazione" (uso, impiego) degli impianti audiovisivi e degli altri strumenti di controllo, richiedendo, per la prima, che venga preventivamente stipulato un accordo sindacale o conseguita l'autorizzazione amministrativa e, per la seconda, che essa risulti orientata esclusivamente alle finalità aziendali indicate dalla norma in maniera tassativa (esigenze organizzative e produttive, sicurezza del lavoro e tutela del patrimonio aziendale). Pertanto, da un lato, l'impiego degli strumenti in questione, come pure l'utilizzazione delle informazioni tramite essi raccolte, sarebbero giustificati solo in presenza delle finalità previste dalla legge, dall'altro, l'accordo sindacale o l'autorizzazione amministrativa dovrebbero necessariamente precedere l'installazione degli strumenti di controllo. Quale ulteriore conseguenza di questa interpretazione[28] è lecito ipotizzare che possano verificarsi casi di installazione degli strumenti di controllo cui non segua un loro effettivo utilizzo per difetto delle esigenze aziendali normativamente indicate, ferma restando la necessità dell'accordo o dell'autorizzazione ai fini della legittimazione dell'installazione.

Il cambiamento d'impostazione della norma, tra la vecchia e la nuova formulazione, potrebbe essere attribuito alla sempre più esplicita commistione tra diritto del lavoro e diritto della privacy e, quindi, alla tendenza di quest'ultimo a ricondurre l'attenzione sulla finalità del trattamento e in particolare sulla disciplina che dovrebbe regolare l'utilizzazione delle informazioni registrate mediante l'uso degli strumenti di controllo[29].

5.2. Dall'elaborazione giurisprudenziale della categoria dei "controlli difensivi" alla previsione normativa della esigenza datoriale di "tutela del patrimonio aziendale"

Una innovazione di molto maggior rilievo rispetto all'originaria formulazione dell'art. 4 dello Statuto è quella introdotta con la riforma del 2015 con riferimento alla previsione normativa delle diverse tipologie di esigenze aziendali considerate idonee a legittimare l'impiego di strumenti per il controllo a distanza dell'attività dei lavoratori. All'interno di queste esigenze datoriali, infatti, oltre alle già considerate "esigenze organizzative e produttive" e alla "sicurezza del lavoro", è ora esplicitamente menzionata la "tutela del patrimonio aziendale".

In questo modo il legislatore, da una parte ha ampliato l'ambito applicativo dei controlli a distanza includendovi anche la finalizzazione alla tutela del patrimonio aziendale, dall'altra ha escluso che possano essere sottratti all'obbligo dell'accordo sindacale o del provvedimento autorizzatorio gli strumenti idonei al controllo a distanza dell'attività dei lavoratori quando il loro impiego sia giustificato da esigenze connesse, appunto, a quella specifica tutela.

In forza dell'innovazione introdotta dall'art. 23 del d.lgs. 151/2015 vengono di fatto a rientrare tra le finalità legittimanti l'impiego di strumenti di controllo anche tutti quei comportamenti del lavoratore che siano comunque suscettibili di determinare effetti pregiudizievoli, oltre che sui singoli beni dell'azienda, anche sulla stessa credibilità e affidabilità dell'impresa, incidendo in misura non trascurabile, anche a livello economico, sul patrimonio aziendale. Anzi, in proposito è da rilevare anche che, all'interno della nozione di "patrimonio aziendale" deve ricomprendersi qualunque bene, di proprietà dell'azienda, che sia comunque necessario alla produzione, sia esso materiale o immateriale[30].

Attraverso le varie forme di comunicazione e interazione realizzabili mediante i social – ma anche mediante la posta elettronica, le conversazioni telefoniche o gli scambi di messaggi, documenti, immagini o filmati (per esempio, via Skype o WhatsApp) – al lavoratore è possibile mettere in atto condotte altamente lesive del patrimonio aziendale, compiendo atti di diffamazione nei confronti dell'imprenditore, furti di dati aziendali, attacchi di spionaggio industriale, ovvero ancora facendo una pubblicità negativa all'impresa o usando – e rendendo conoscibili a un pubblico indefinito – espressioni offensive od infamanti nei confronti del datore di lavoro.

Con la riconosciuta esigenza di tutela del patrimonio aziendale, però, è concettualmente ammissibile porre in rapporto la reazione del datore di lavoro non solo nei confronti dei comportamenti illeciti del lavoratore (eventualmente messi in atto mediante l'uso di social network), ma anche di fronte a condotte che, pur non configurandosi come illecite, comportino comunque la sottrazione di tempo all'attività lavorativa, costituendo inadempimento della prestazione principale. Così, il dipendente che, durante l'orario di lavoro, dedichi la sua attenzione nell'intrattenere rapporti su una piattaforma social, pur non compiendo un atto illecito, non si potrebbe sicuramente sostenere che adempia correttamente all'obbligo della prestazione di cui il datore di lavoro è creditore.

Per tal via, però, comportamenti illeciti e comportamenti inadempienti del lavoratore – nell'ambito della trattazione qui svolta, rilevanti con riferimento all'impiego strumentale dei social network – verrebbero a essere legittimamente considerati entrambi come lesivi del patrimonio aziendale e, quindi, come possibile oggetto di controllo da parte del datore di

lavoro, in funzione tanto reattiva che preventiva. Da una parte, infatti, è innegabile che la prestazione lavorativa abbia un contenuto patrimoniale e che il suo puntuale adempimento concorra alla valorizzazione del patrimonio aziendale, per cui si potrebbe ritenere che all'interno dell'esigenza di tutela del patrimonio aziendale sia ricompresa anche quella di accertare il corretto adempimento della prestazione lavorativa di cui è creditore l'imprenditore; dall'altra, però, è evidente anche che, con la nuova formulazione dell'art. 4 dello Statuto, il legislatore non si è certo proposto di abolire il divieto di controlli a distanza sull'attività lavorativa, esplicitamente sancito nel testo originario.

In proposito si rileva che, in un comunicato del 2018[31], il Ministero del lavoro e delle politiche sociali ha ritenuto di dover fornire precisazioni sui controlli a distanza dopo il Jobs Act, a seguito delle affermazioni riportate dalle agenzie di stampa secondo le quali questa legge di riforma del mercato del lavoro avrebbe autorizzato l'utilizzo di dispositivi per il controllo a distanza dei lavoratori. Secondo quanto dichiarato nel comunicato in questione, l'intento del legislatore sarebbe stato, invece, non quello di "liberalizzare" i controlli, bensì di fare «chiarezza circa il concetto di 'strumenti di controllo a distanza' e i limiti di utilizzabilità dei dati raccolti attraverso questi dispositivi, in linea con le indicazioni che il Garante della privacy ha fornito negli ultimi anni». La modifica apportata dall'art. 23, d.lgs. 151/2015 all'art. 4, l. 300/1970 avrebbe, quindi, confermato che questi strumenti possono essere adottati «esclusivamente previo accordo sindacale o autorizzazione dell'Ispettorato Territoriale del Lavoro o del Ministero».

Da parte sua l'Ispettorato, con la Circolare n. 5 del 19 febbraio 2018, ricollegandosi a quanto introdotto in materia dall'art. 23 del dlgs. n. 151/2015 e dall'art. 5, co. 2, del d.lgs. n. 185/2016, ha formulato indicazioni operative sull'installazione e l'utilizzo di impianti audiovisivi e di altri strumenti di controllo ai sensi dell'art. 4 della legge n. 300/1970. Ferma restando la documentazione che i datori di lavoro sono tenuti a presentare per ottenere l'autorizzazione a installare telecamere o, in genere, strumenti comunque utilizzabili per il controllo a distanza dell'attività dei lavoratori, si precisa che la valutazione delle istanze deve essere concentrata sull'effettiva sussistenza delle ragioni che legittimano l'adozione del provvedimento, tenendo soprattutto presenti le finalità per cui la singola autorizzazione è richiesta (ragioni organizzative e produttive, sicurezza sul lavoro e tutela del patrimonio aziendale). Sussistendo le ragioni giustificatrici del controllo, nella Circolare si ammette la possibilità d'inquadrare direttamente il lavoratore, in via incidentale e con carattere di occasionalità, ma senza condizioni e limiti predeterminati. In particolare, la visione delle immagini in tempo reale da postazione remota è dichiarata ammissibile solo in casi eccezionali e debitamente motivati, mentre, per quanto riguarda le esigenze di tutela del "patrimonio aziendale", si richiede che la relativa nozione, proprio per la sua ampiezza, venga in concreto adeguatamente declinata e precisata, tenendo sempre presenti i principi di legittimità e determinatezza del fine perseguito, nonché della sua proporzionalità, correttezza e non eccedenza. In base a tali principi i controlli più invasivi sarebbero pertanto da legittimare solo a fronte della rilevazione di specifiche anomalie e, comunque, all'esito dell'esperimento di misure preventive meno limitative dei diritti dei lavoratori. È invece vietata l'utilizzazione di apparecchiature di videosorveglianza installate, ma non ancora messe in funzione, come pure l'installazione di telecamere finte, montate a scopo dissuasivo.

Più di recente, poi, con la Lettera Circolare del 18 giugno 2018 prot. n. 302, contenente "Indicazioni operative sul rilascio dei provvedimenti autorizzativi ai sensi dell'art. 4 della legge n. 300/1970", l'Ispettorato Nazionale del Lavoro ha chiarito che le richieste di autorizzazione indirizzate dalle imprese all'Ispettorato e alle sue strutture territoriali in ordine all'installazione di impianti audiovisivi e di altri strumenti dai quali possa derivare un controllo a distanza dell'attività dei lavoratori, devono essere corredate dagli estratti del documento di valutazione dei rischi (DVR).

Inoltre, il Dicastero ha precisato che l'attuale assetto normativo intende tutelare «ancor meglio rispetto al passato, la posizione del lavoratore, imponendo che al lavoratore venga data comunque adeguata informazione circa l'esistenza e le modalità d'uso di strumenti di lavoro che possano consentire un controllo a distanza». Questa ultima osservazione si collega alla utilizzabilità delle informazioni raccolte ai sensi dei co. 1 e 2, art. 4, ma il testo normativo (co. 3) più analiticamente dichiara che tali informazioni sono utilizzabili a tutti i fini connessi al rapporto di lavoro (quindi anche a fini disciplinari), a condizione, però, 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 decreto legislativo 30 giugno 2003, n. 196»[32].

Mentre il secondo elemento della condizione si ricollega alla vastissima problematica della tutela dei dati personali, il primo rinvia alla *social media policy*, come documento di valore legale con cui, in genera-

le, i responsabili dell'impresa regolano le relazioni, mediate appunto dai social, tra l'azienda e i suoi dipendenti (*social media policy* interna), da una parte, e tra l'azienda e i suoi clienti/utenti (*social media policy* esterna), dall'altra.

Il profilo social o la pagina web di un'azienda sono principalmente rivolti all'esterno, prendendo soprattutto in considerazione gli obiettivi produttivi (target), le possibili esigenze della clientela potenziale (*prospect client*), gli interessi dei diversi soggetti – individui od organizzazioni – a vario titolo attivamente coinvolti nell'iniziativa economica (c.d. stakeholders: clienti; fornitori; altre organizzazioni eventualmente implicate nel rapporto tra clienti e fornitori; finanziatori; fruitori dei risultati dell'attività aziendale; gruppi d'interesse locali, considerati in relazione all'ambiente in cui l'attività si sviluppa e realizza i suoi risultati). Pertanto, una *social media policy* esterna ha per oggetto l'indicazione delle finalità dell'azienda, della tipologia dei contenuti pubblicati e, in generale, dei comportamenti non accettati (come spam; off-topics (OT); commenti offensivi ovvero espressioni volgari o violente nei confronti di chi gestisce il social, di altri clienti/utenti o di appartenenti a minoranze etniche, politiche o religiose; invio di messaggi provocatori e irritanti (*trolling*), ovvero ostili, aggressivi e opprimenti (*flaming*); iniziative volte a promuovere o sostenere attività illegali, diffamanti o minacciose; violazioni del diritto d'autore; utilizzo non autorizzato di marchi registrati; diffusione di dati personali riservati). In caso di trasgressione delle regole indicate viene precisato il sistema sanzionatorio applicabile, mentre, per i casi più gravi, è fatto rinvio al necessario ricorso all'autorità giudiziaria.

Tuttavia, in considerazione del fatto che nessuno conosce l'azienda, la sua realtà e i suoi problemi, meglio del personale che vi lavora, a fianco della *social media policy* esterna, si tende attualmente a riconoscere una rilevante importanza pratica anche a quella interna. In essa, di regola, sono indicati gli obiettivi della strategia social da perseguire, ma sono anche specificate le tipologie d'informazioni aziendali che possono o devono essere condivise, sono forniti esempi dei contenuti per i quali è richiesta l'approvazione prima della pubblicazione e sono esplicitate le modalità d'utilizzo del logo aziendale o di altre informazioni comunque relative al brand dell'impresa. In generale, la *social media policy* interna si presenta come un documento volto a sensibilizzare il personale, informandolo sull'uso corretto dei social media con riferimento sia al rapporto di lavoro con l'azienda, sia ai discorsi (pareri, opinioni, giudizi) eventualmente espressi su di essa. In questo senso i dipendenti vengono a disporre di una guida condivisa, di una specie di manuale di comportamento, contenente l'indicazione delle regole (con le relative sanzioni) e delle buone prassi cui attenersi al fine di svolgere correttamente l'attività lavorativa, evitando di commettere errori o veri e propri illeciti potenzialmente dannosi nei confronti dell'impresa, ma avendo anche la possibilità di tutelarsi nei confronti di eventuali abusi nell'esercizio datoriale del potere di controllo.

Un profilo diverso rispetto ai contenuti fin qui indicati – tutti relativi ai comportamenti imposti (ma, talvolta, solo consigliati o suggeriti) dal datore di lavoro al lavoratore relativamente all'impiego dei social network – è quello che invece attiene all'adeguata informazione che l'imprenditore deve dare al dipendente relativamente alle «modalità d'uso degli strumenti e di effettuazione dei controlli», di cui al già citato co. 3, art. 4, st. lav.

5.3. Il secondo comma del nuovo art. 4 e la distinzione tra "strumenti di controllo" e "strumenti di lavoro"

Proprio in ragione delle loro peculiari funzionalità i social network possono essere utilizzati da parte del lavoratore come veri e propri strumenti di lavoro. Può accadere, infatti, che il lavoratore utilizzi una piattaforma social per eseguire la sua prestazione lavorativa, ad esempio in ordine alla realizzazione di strategie di marketing aziendali che comportino campagne pubblicitarie e promozionali, ovvero per la gestione dei reclami o delle richieste degli utenti. In tutte queste ipotesi, trattandosi in sostanza di utilizzare un profilo social aziendale, con "account" e credenziali di accesso forniti dall'impresa, i problemi connessi a un'eccessiva invadenza del controllo datoriale possono risultare di non agevole soluzione.

Di certo, in base all'art. 4 della legge n. 300/1970 – e, in particolare, in ragione del combinato disposto dei commi 2 e 3 – il datore di lavoro può monitorare l'utilizzo del social da parte del proprio dipendente allo scopo di verificare se il profilo social assegnato (inteso qui come strumento di lavoro smaterializzato, in quanto accessibile da qualunque dispositivo e in qualunque luogo e, quindi, operativo anche a prescindere dall'uso di un computer dell'impresa) sia effettivamente utilizzato per eseguire la prestazione contrattualmente richiesta e nel rispetto delle direttive aziendali. Di conseguenza, l'eventuale constatazione di un utilizzo improprio dello strumento di lavoro in questione – per esempio, nel caso in cui si accerti che il lavoratore, in orario di lavoro, si intrattenga in chat con amici e conoscenti tramite il profilo social aziendale o lo adoperi per fare pubblicità a pro-

dotti di terzi – può legittimare l'esercizio dei poteri disciplinari, fino a determinare il licenziamento.

Tuttavia se, da una parte, l'assegnazione al lavoratore del profilo social aziendale, in quanto necessaria premessa all'utilizzo del social a fini lavorativi, può avvenire senza vincoli sostanziali e procedurali in un regime di semplificazione rispondente all'interesse dell'impresa, dall'altra, l'attività di controllo datoriale deve intendersi, invece, rigorosamente subordinata al rispetto di precisi limiti, specificamente derivanti dalla natura di "dati sensibili" attribuibile alle informazioni personali che lo strumento tecnologico memorizza e rende disponibili. Di conseguenza, in tanto il datore di lavoro potrà legittimamente utilizzare le informazioni raccolte all'esito della sua attività di controllo, in quanto tale verifica si sia svolta con l'osservanza delle disposizioni dettate dall'ordinamento in materia di tutela della riservatezza (Codice della privacy e provvedimenti del Garante), e quindi nel rispetto dei principi di trasparenza (con il corollario dell'obbligo di informativa su modi e forme di controllo), di necessaria proporzionalità e di prevenzione.

È, in particolare, l'obbligo d'informativa attraverso la normativa interna ad assumere rilievo, imponendosi al datore di lavoro di comunicare preventivamente al lavoratore come e quando potrà e dovrà utilizzare il profilo aziendale, chiarendo che la relativa attività potrà essere monitorata a distanza, fermo restando che, in base all'obbligo di prevenzione, il controllo successivo sul singolo lavoratore potrà costituire soltanto una misura estrema, destinata a trovare attuazione esclusivamente nell'ipotesi in cui, all'esito di controlli aggregati che non implichino l'accesso ai dati individuali (ad esempio relativi alle spese per l'utenza o ai tempi di accesso), si riscontri la necessità di procedere in questo senso. In tal caso, comunque, dovrà osservarsi il principio di necessaria proporzionalità, in forza del quale sarà esclusa la possibilità di "controlli prolungati continui e indiscriminati".

6. Social network e tutela della privacy del lavoratore

È evidente che la materia del controllo dell'attività dei lavoratori trovi un suo limite coessenziale nella tutela della riservatezza dei medesimi. A tale riguardo, volendo sinteticamente illustrare lo stato dell'arte sul punto, occorre segnalare che il gruppo di studio "Articolo 29" [33], ha ridefinito il quadro europeo dei principi fondamentali in materia con il parere n. 2 dell'8 giugno 2017 (*Opinion 2/2017 on data processing at work*), aggiornandolo ai progressi tecnologici e, dunque, anche al nuovo ruolo che i social network hanno assunto nel contesto lavorativo e sociale in genere[34].

Secondo il documento redatto dal gruppo di studio "Articolo 29"[35] sarà possibile effettuare controlli al fine di evitare la fuga di dati relativi all'attività dell'impresa o la compromissione dei sistemi informatici aziendali. Il datore di lavoro non potrà, però, "spiare" le comunicazioni dei dipendenti, per cui l'eventuale consultazione dei social network cui essi partecipino dovrà essere strettamente limitata ai loro profili professionali. Inoltre, al lavoratore dovranno essere offerti spazi privati e servizi cloud sui computer aziendali[36].

Il documento in questione tiene conto sia della normativa previgente sia delle novità introdotte dal Regolamento UE 2016/679 (GDPR - *General Data Protection Regulation*)[37], applicabile a decorrere dal mese di maggio 2018. Oltre a definire i principi generali, esso fornisce esempi concreti per il corretto trattamento dei dati in ambito professionale. L'assunto fondamentale è quello per cui il lavoratore, indipendentemente dal contratto a lui applicato, ha diritto al rispetto della sua vita privata, della sua libertà e dignità. Soprattutto nelle ipotesi in cui, in osservanza delle normative nazionali, siano previste forme di controllo sulla sua attività, egli dovrà essere informato sulle modalità di trattamento dei suoi dati personali in maniera chiara, semplice ed esaustiva, secondo un rigido principio di trasparenza, che trova pratica attuazione nella predisposizione datoriale di norme regolamentari interne.

Secondo quanto osservato dal citato organo consultivo europeo, tenendo conto della posizione di subordinazione, anche psicologica, del lavoratore rispetto al datore di lavoro – titolare, nei suoi confronti, non solo del potere direttivo, che si esplica con la formulazione di istruzioni per lo svolgimento della prestazione, ma anche del potere di controllo, espresso mediante la verifica dell'attività lavorativa svolta, e del potere disciplinare che si esercita mediante l'irrogazione di sanzioni in caso d'inadempimento della prestazione –, difficilmente il consenso del lavoratore potrà configurarsi come condizione di per sé adeguata e sufficiente a fondare la legittimità dell'utilizzo dei suoi dati. Il datore di lavoro, quindi, in alternativa, potrà valutare l'opportunità di ricorrere a quanto specificamente previsto in disposizioni normative o contrattuali o far valere il proprio "legittimo interesse", per esempio, alla sicurezza e alla corretta allocazione delle risorse.

Il necessario bilanciamento tra l'interesse del datore di lavoro, da una parte, e i diritti e le libertà del

lavoratore, dall'altra, dovrà però avvenire in conformità ai principi di necessità e proporzionalità: l'uso dei dati personali deve essere limitato il più possibile e ogni trattamento deve risultare proporzionato alla finalità perseguita, oltre che – come già precisato – espressamente disciplinato da regolamenti aziendali conformi alle norme vigenti.

In applicazione dei suddetti principi di rispetto della riservatezza, della libertà e della dignità del lavoratore, di salvaguardia del suo consenso alla raccolta ed al trattamento dei suoi dati e di proporzionalità e trasparenza, il gruppo di studio "Articolo 29" aveva quindi dettato le seguenti indicazioni relative alle modalità di controllo consentite.

I Garanti pongono in evidenza come, pur essendo possibile, per il datore di lavoro, introdurre strumenti e tecnologie per ridurre il rischio di attacchi informatici o della diffusione di informazioni riservate, resta però fermo il divieto di sottoporre a sorveglianza la posta elettronica dei dipendenti o controllare la loro navigazione in Internet. Anche in queste ipotesi dovrebbero essere privilegiate misure preventive, assolutamente trasparenti, atte a segnalare in anticipo la possibilità della violazione.

Per quanto specificamente riguarda i social network, l'eventuale consultazione o il monitoraggio devono essere limitati ai soli profili professionali, escludendo rigidamente quanto possa attenere alla vita privata di dipendenti o candidati all'assunzione e ciò a tutela del diritto fondamentale a non essere oggetto di discriminazione sulla base delle proprie idee politiche o religiose, del proprio impegno sociale o di altri aspetti della propria vita personale o familiare[38].

Infine, allo scopo di favorire il corretto utilizzo degli strumenti e delle policy aziendali, i Garanti invitano i datori di lavoro a offrire ai dipendenti connessioni Wi-Fi distinte da quelle utilizzate per l'attività lavorativa, oltre a spazi digitali riservati – su computer, smartphone, cloud e posta elettronica – in cui possano essere conservati documenti o inviate comunicazioni personali, non accessibili a persone diverse dai diretti interessati se non in casi assolutamente eccezionali.

Si tratta in larga parte di principi e regole già ampiamente condivisi e fatti propri nel nostro ordinamento da parte del Garante per la protezione dei dati personali con le linee guida del 1° marzo 2007, e da questo ribaditi a più riprese nel corso degli anni successivi. Così è stato, ad esempio, anche nel provvedimento del 13 giugno 2016, in cui il Garante della Privacy è nuovamente intervenuto sul tema dei poteri di controllo del datore di lavoro sugli strumenti informatici dei dipendenti, per ribadire la contrarietà al Codice della Privacy e allo Statuto dei lavoratori dei controlli indiscriminati sulla posta elettronica e sulla navigazione in Internet dei dipendenti, secondo un'impostazione che è rimasta immutata anche a seguito dell'entrata in vigore dell'art. 4 dello Statuto dei lavoratori, come riformato dal Jobs Act[39]. Del resto, proprio il nuovo comma terzo della suddetta disposizione, nel fissare i limiti essenziali all'utilizzabilità dei dati acquisiti dal datore di lavoro in sede di controllo, richiama ora espressamente le norme dettate in modo specifico a salvaguardia della riservatezza, stabilendo che «le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili 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 decreto legislativo 30 giugno 2003, n. 196»[40].

Per quanto in questa sede maggiormente rileva – in relazione, cioè, alla possibilità da parte del datore di lavoro di utilizzare i social network in funzione di controllo –, occorre senz'altro evidenziare, sul piano formale, che il recente documento di fonte europea sicuramente valorizza in modo inedito i social network, riconoscendo ad essi una rilevanza testuale specifica e autonoma.

A decorrere dal 25 maggio 2018 ha trovato piena attuazione, come detto, il GDPR. Avendo ad oggetto la protezione delle persone fisiche relativamente al trattamento dei dati personali, nonché alla libera circolazione di tali dati, esso abroga la Direttiva 95/46/CE e fornisce numerose disposizioni in materia di raccolta, archiviazione e gestione in sicurezza dei dati personali, introducendo sostanziali novità e nuovi ruoli di responsabilità, con sanzioni che risultano fortemente inasprite e, in determinate situazioni, prevedono anche conseguenze penali. In particolare, le immagini riprese con sistemi di videosorveglianza sono equiparate ai dati personali e come tali sono regolamentate.

Il 19 settembre 2018, poi, è entrato in vigore il d.lgs. 10 agosto 2018, n. 101, pubblicato sulla Gazzetta Ufficiale n. 205 del 4 settembre 2018 e contenente disposizioni per l'adeguamento della normativa nazionale (cioè del Codice in materia di protezione dei dati personali - d.lgs. 196/2003) al Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio, del 27 aprile 2016.

Sul piano sostanziale, poi, in merito alla limitazione del controllo ai soli profili professionali del lavoratore, di certo questo non potrà significare che al datore di lavoro sia in assoluto precluso l'accesso alle informazioni e ai contenuti che i propri dipendenti condividono in rete. Quei contenuti, infatti, se non filtrati per il tramite di password o comunque di au-

torizzazioni specifiche da parte dell'interessato, oppure veicolati a mezzo di messaggi privati, o ancora condivisi tra una cerchia ristretta di internauti (specie se tutti interni all'azienda, e sempre che nessuno di questi abbia divulgato quel materiale a terzi, tanto meno in rete), sono e restano accessibili da parte di tutti gli utenti e, dunque, anche da parte del datore di lavoro, che potrà trarne informazioni a proposito del rispetto da parte del lavoratore degli obblighi impostigli dal rapporto di lavoro e, in particolare, del dovere di fedeltà.

Con il Provvedimento n. 53 del 1° febbraio 2018 il Garante della privacy ha dichiarato illecito il comportamento adottato da molti datori di lavoro al fine di conservare in maniera sistematica i messaggi di posta elettronica che i dipendenti si scambiano attraverso gli account aziendali. Nel caso di specie il Garante ha osservato, in particolare, che sarebbe stato violato l'obbligo d'informativa previsto dall'art. 13 del d.lgs. n. 196/2003, in quanto la società non avrebbe adeguatamente informato i dipendenti in merito alle modalità e finalità dell'attività di raccolta e conservazione dei dati relativi all'utilizzo della posta elettronica. In secondo luogo, la conservazione metodica di tutte le comunicazioni scambiate dai dipendenti attraverso gli account aziendali in vista di futuri ed eventuali contenziosi si porrebbe in contrasto coi principi di liceità, necessità e proporzionalità del trattamento dei dati di cui agli artt. 3 e 11 del decreto sopra citato. Soprattutto, però, interessa qui rilevare che la raccolta sistematica delle comunicazioni elettroniche in transito sugli account aziendali dei dipendenti in servizio, la loro memorizzazione per un periodo predeterminato e comunque ampio, insieme alla possibilità per il datore di lavoro di accedervi per finalità indicate in astratto e in termini generali, si è ritenuto consentissero alla società di effettuare un vero e proprio controllo a distanza dell'attività dei dipendenti, risultando perciò – in assenza di procedura autorizzativa – in contrasto con la disciplina di settore prevista dall'art. 4 dello Statuto dei lavoratori.

Questo è, però, un piano diverso e distinto da quello del controllo datoriale sull'attività lavorativa: concerne, sì, l'impiego dei social da parte dei lavoratori, ma sotto il profilo della rilevanza giuslavoristica dei comportamenti extralavorativi del lavoratore e non dell'uso che questo faccia di tali strumenti di comunicazione e condivisione di massa durante l'orario di lavoro[41].

In tale ultimo caso, più specificamente, la limitazione del controllo in senso stretto ai soli profili professionali del lavoratore appare poco congrua, potendosi spingere il suo significato fino al punto di ritenere legittimo – o meglio non monitorabile – l'utilizzo da parte del lavoratore di social network attraverso il proprio profilo privato durante l'orario di lavoro, magari attraverso l'utilizzo di computer o telefoni aziendali. Una simile soluzione sarebbe evidentemente errata, dovendo coordinarsi il predetto riferimento, in modo sistematico, con le disposizioni normative vigenti, che sanciscono l'obbligo di diligenza del lavoratore nell'esecuzione della prestazione lavorativa, *ex* art. 2104 c.c., e, se del caso, con il divieto di utilizzare gli strumenti dell'impresa a scopo privato. Semmai, il necessario rispetto del principio di trasparenza nell'effettuazione dei controlli, con il corollario della predeterminazione nella normativa interna degli strumenti e delle forme di monitoraggio (ormai peraltro già stabilito anche a livello normativo, dopo il Jobs Act), sembra precludere al datore di lavoro avventurosi e fantasiosi escamotage (come la creazione di profili fake sui social) pur di cogliere in fallo i propri dipendenti, con buona pace della loro riservatezza (e ammesso e non concesso che, in quei casi, di prioritaria salvaguardia della riservatezza sia lecito parlare).

7. Conclusione

A conclusione – sia pur parziale e sommaria – dell'indagine fin qui svolta è opportuno rilevare che il complesso contesto normativo (e giurisprudenziale) che si è venuto a formare intorno alla formulazione novellata dell'art. 4 dello Statuto dei lavoratori è stato ispirato dall'esigenza avvertita dal legislatore di rivedere la materia dei «controlli a distanza sugli impianti e sugli strumenti di lavoro, tenendo conto dell'evoluzione tecnologica e contemperando le esigenze produttive ed organizzative dell'impresa con la tutela della dignità e riservatezza del lavoratore»[42].

Già la formulazione del dettato normativo era apparsa vaga e imprecisa agli interpreti, non lasciando intravedere le linee portanti dell'annunciata riforma. Tuttavia – come è stato da più parti osservato –, proprio in considerazione della vitalità del meccanismo introdotto con la normativa statutaria, tenendo conto dell'evoluzione tecnologica intervenuta, si sarebbe potuto chiarire definitivamente l'ambito di applicazione dell'art. 4, esplicitando la natura e la portata degli strumenti di controllo nella loro attuale configurazione, fortemente caratterizzata nel senso della molteplicità e diversità delle funzioni esplicabili, nell'ambito dello svolgimento della prestazione lavorativa come in quello dell'attuazione dell'attività datoriale di controllo.

Da una parte, infatti, risulta evidente che alla rapidità e imprevedibilità del progresso tecnologico e

delle sue concrete applicazioni nella vita sociale come nel mondo del lavoro inevitabilmente si contrappongono quelle connotazioni di lentezza, improvvisazione e provvisorietà che purtroppo sovente ineriscono agli interventi del legislatore. Sotto un diverso profilo, però, proprio in ragione della velocità con cui in questi ultimi anni si assiste a veri e propri cambiamenti epocali, si deve comunque ammettere che sia in qualche modo prevedibile la produzione di norme fin dall'inizio obsolete.

In margine a questa breve riflessione merita forse accennare alle insospettate dimensioni dei fenomeni collegati alla realtà dei social network nel senso della profonda incidenza che essi possono avere, influenzando persino l'evoluzione del contesto politico e il corso della storia: si allude – com'è evidente – al recente scandalo in cui sono rimasti coinvolti un'azienda di consulenza per il marketing online e il più noto dei social network mondiali[43].

Note

[1]Il termine coniato per designare questa nuova realtà è *Wikinomics*, tratto dal titolo di un famoso libro di D. Tapscott, A.D. Williams, *How Mass Collaboration Changes Everything*, New York, Portfolio, 2006; (I ed. italiana: *Wikinomics. La collaborazione di massa che sta cambiando il mondo*, Milano, Etas Kompass, 2007).

[2]In particolare, Facebook dispone di due tipologie di servizi social, con finalità nettamente distinte: il "profilo personale" (diario) e la "pagina pubblica" (Facebook *for business*).

[3]Nel mondo di Facebook, a partire dal febbraio 2016, al semplice "like" (il pulsante like è stato definito «il più famoso tasto del Web») si sono affiancate le *reaction*, che consentono agli utenti del servizio di interagire in modo più articolato e soddisfacente.

[4]Così si esprime la l. 10 dicembre 2014, n. 183, all'art. 1, co. 7, lett. *f*).

[5]L'elaborazione dottrinale formatasi sui problemi interpretativi posti dall'art. 4 dello Statuto dei lavoratori è molto ampia. Senza pretesa di completezza, richiamandoci ad alcuni contributi recenti contenenti accurate ricostruzioni di tale dibattito si vedano, tra gli altri: A. Ingrao, *Il controllo a distanza sui lavoratori e la nuova disciplina privacy. Una lettura integrata*, Bari, Cacucci, 2018, 256 p.; I. Seghezzi, *I social network e le nuove frontiere dell'illecito disciplinare*, in "Il lavoro nella giurisprudenza", 2018, n. 6, p. 556; P. Tullini (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Torino, Giappichelli, 2017, 225 p.; C. Gamba, *Il controllo a distanza delle attività dei lavoratori e utilizzabilità delle prove*, in "Labour & Law Issues", 2016, vol. 2, n. 1, p. 120; A. Levi (a cura di), *Il nuovo art. 4 sui controlli a distanza. Lo Statuto dei lavoratori dopo il Jobs Act*, Milano, Giuffrè, 2016, 194 p.; M.T. Carinci, *Il controllo a distanza dell'attività dei lavoratori dopo il "Jobs Act" (art. 23 D. Lgs. 151/2015): spunti per un dibattito*, in "Labour & Law Issues", 2016, vol. 2, n. 1, 14 p.; M. Marazza, *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore)*, WP C.S.D.L.E. "Massimo D'Antona", IT - 300/2016; G. Fava, *Privacy e controllo dei lavoratori alla luce del Jobs Act*, Guerini Next, 2016, 251 p.; 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)*, WP C.S.D.L.E. "Massimo D'Antona", IT n. 255/2015; A. Minervini, *I controlli sul lavoratore e la tutela dell'azienda*, in "Il lavoro nella giurisprudenza", 2014, n. 4, p. 314; A. Levi, *Il controllo informatico sull'attività del lavoratore*, Torino, Giappichelli, 2013, 225 p.; M. Miscione, *I controlli intenzionali, preterintenzionali e difensivi sui lavoratori in contenzioso continuo*, in "Il lavoro nella giurisprudenza", 2013, n. 8-9, p. 761; A. Trojsi, *Il diritto del lavoratore alla protezione dei dati personali*, Torino, Giappichelli, 2013; P. Tullini (a cura di), *Tecnologie della comunicazione e riservatezza nel rapporto di lavoro. Uso dei mezzi elettronici, potere di controllo e trattamento dei dati personali*, in "Trattato di diritto commerciale e diritto pubblico dell'economia", diretto da F. Galgano, Cedam, 2010, 194 p.; M.T. Salimbeni, *Il controllo a distanza sull'attività dei lavoratori: la sopravvivenza dell'art. 4 sugli impianti audiovisivi*, in "Diritto, Lavoro, Mercati", 2010, n. 3, p. 587; C. Zoli, *Il controllo a distanza del datore di lavoro: l'art. 4, l. n. 300/1970 tra attualità ed esigenze di riforma*, in "Rivista italiana di diritto del lavoro", 2009, n. 4, pp. 485-503; M. Aimo, *Privacy, libertà di espressione e rapporto di lavoro*, Napoli, Jovene, 2003, X-390 p.; C. Assanti, G. Pera, *Art. 4 (Impianti audiovisivi)*, in C. Assanti, G. Pera (a cura di), "Commento allo Statuto dei diritti dei lavoratori", Cedam, 1972, 450 p.

[6]Ai sensi di quanto disposto dall'art. 43, co. 1 dello stesso d.lgs. 151/2015.

[7]Ai sensi di quanto disposto dall'art. 6, co. 1, del medesimo d.lgs. 185/2016.

[8]Il d.lgs. 24 settembre 2016, n. 185, contiene le disposizioni integrative e correttive apportate ai cinque decreti legislativi emanati in attuazione della legge delega 10 dicembre 2014, n. 183 (c.d. "Jobs Act"), cioè ai d.lgs. 15 giugno 2015, n. 81 e 14 settembre 2015, nn. 148-151.

[9]Come è noto, si tratta della l. 183, 10 dicembre 2014 - *Deleghe al Governo in materia di riforma degli ammortizzatori sociali, dei servizi per il lavoro e delle politiche attive, nonché in materia di riordino della disciplina dei rapporti di lavoro e dell'attività ispettiva e di tutela e conciliazione delle esigenze di cura, di vita e di lavoro (14G00196)*.

[10]Si veda E. Barraco, A. Sitzia, *Potere di controllo e privacy. Lavoro, riservatezza e nuove tecnologie*, Milano, Wolters Kluwer, 2016, p. 6.

[11]Si veda M.T. Carinci, *op. cit.*, p. 3; R. Del Punta, *La nuova disciplina dei controlli a distanza sul lavoro (art. 23 d.lgs. n. 151/2015)*, in "Rivista italiana di diritto del lavoro", 2016, n. 1, p. 96; P. Lambertucci, *op. cit.*

[12]Per la definizione giurisprudenziale dei controlli difensivi come «controlli diretti ad accertare condotte illecite del lavoratore» si vedano, tra l'altro, Cass. 4 aprile 2012, n. 5371 e Cass. 23 febbraio 2012, n. 2722, in "Rivista italiana di diritto del lavoro", 2013, II, 113.

[13]Si veda Cass. 3 aprile 2002, n. 4746, in "Rivista giuridica del lavoro e della previdenza sociale", 2002, 642 e in "Massimario di giurisprudenza del lavoro", 2002, 644. Nella sentenza la Corte aveva affermato che «ai fini dell'operatività del divieto di utilizzo di apparecchiature per il controllo a distanza dell'attività dei lavoratori previsto dall'art. 4 della l. 300/1970, è necessario che il controllo riguardi (direttamente o indirettamente) l'attività lavorativa, mentre devono ritenersi certamente fuori dell'ambito di applicazione della norma i controlli diretti ad accertare condotte illecite del lavoratore (cosiddetti controlli difensivi), quali, ad esempio, i sistemi di controllo dell'accesso ad aree riservate o, appunto, gli apparecchi di rilevazione di telefonate ingiustificate».

[14]Si vedano, tra gli altri, P. Tullini, *Comunicazione elettronica, potere di controllo e tutela del lavoratore*, in "Rivista italiana di diritto del lavoro", 2009, n. 3, p. 323; C. Zoli, *Il controllo a distanza del datore di lavoro: l'art. 4, l. n. 300/1970 tra attualità ed esigenze di riforma*, in "Rivista italiana di diritto del lavoro", 2009, n. 4, p. 500; A. Bellavista, *La Cassazione e i controlli a distanza sui lavoratori*, in "Rivista giuridica del lavoro e della previdenza sociale", 2010, n. 3, p. 462.

[15]Una sintesi dei principali orientamenti assunti dalla giurisprudenza di merito sulla questione è in M.L. Vallauri, *È davvero incontenibile la forma espansiva dell'art. 4 dello Statuto dei lavoratori?*, in "Rivista italiana di diritto del lavoro", 2008, n. 3, p. 718.

[16]Reperibile in "Rivista giuridica del lavoro e della previdenza sociale", 2008, p. 714. La Corte affermò che l'art. 4 dello Statuto «fa parte di quella complessa normativa diretta a contenere in vario modo le manifestazioni del potere organizzativo e direttivo del datore di lavoro che, per le modalità di attuazione incidenti nella sfera della persona, si ritengono lesive della dignità e della riservatezza del lavoratore [...] sul presupposto – espressamente precisato nella Relazione ministeriale – che la vigilanza sul lavoro, ancorché necessaria nell'organizzazione produttiva, vada mantenuta in una dimensione umana, e cioè non esasperata dall'uso di tecnologie che possono rendere la vigilanza stessa continua e anelastica, eliminando ogni zona di riservatezza e di autonomia nello svolgimento del lavoro».

[17]Si veda Cass., 23 febbraio 2010, n. 4375, in "Rivista italiana di diritto del lavoro", 2010, n. 3, pt. II, p. 564, con nota di R. Galardi. Si veda anche S. Barone, *Il controllo datoriale a distanza: disciplina vigente e nuove frontiere tecnologiche*, in "Altalex", 15 luglio 2010.

[18]Si veda Cass. 1° ottobre 2012, n. 16622, in "Il Foro italiano", 2012, I, c. 3328. Per un breve commento si veda G. Tripodi, *Vietato usare le registrazioni delle telefonate per licenziare un operatore call center*, in "Sentenze-Cassazione.com", 5 ottobre 2012.

[19]Si veda N.M. Salvi, *Controlli a distanza e consenso dei lavoratori: la Cassazione fa dietrofront*, in "Altalex", 10 maggio 2017; L. Failla, *È reato installare strumenti di controllo a distanza dell'attività dei lavoratori, anche in presenza di un accordo sottoscritto da tutti i dipendenti*, in "Diritto24", 18 maggio 2017.

[20]Reperibile in "Il Foro italiano", 2012, I, c. 1421; anche in "Lavoro nella giurisprudenza", 2012, n. 5, p. 507. Per un inquadramento della sentenza in questione nell'ambito dei diversi orientamenti giurisprudenziali si veda C. Gamba, *op. cit.*, p. 136.

[21]Sul tema si vedano, tra gli altri, D. Bellini, *Controlli difensivi: è legittimo il licenziamento del lavoratore che gioca con il computer aziendale*, in "Labor. Il lavoro nel diritto", 12 giugno 2018; G. Bulgarini D'Elci, *I pc dei dipendenti sono controllabili*, in "Il Sole24ore.com", 28 maggio 2018.

[22]Per il testo completo dell'ordinanza si può consultare http://www.rivistalabor.it. Un commento è in R. Maraga, *Utilizzabilità dei dati raccolti tramite l'uso di strumenti tecnologici da parte del dipendente: gli orientamenti della giurisprudenza*, in "Il Giuslavorista", 14 novembre 2018.

[23]Si veda Cass., sez. lav., 27 maggio 2015, n. 10955; anche in "Il Foro italiano", 2015, I, c. 2316. La notevole risonanza della sentenza in questione è testimoniata anche dalla presenza di pregevoli note e commenti all'interno di numerosi siti.

[24]Sullo specifico punto della localizzazione del dipendente avvenuta in conseguenza del suo accesso a Facebook, la Suprema Corte ha rilevato che, secondo un consolidato orientamento della giurisprudenza di legittimità, l'attività di indagine volta a seguire i movimenti di un soggetto e a localizzarlo attraverso il GPS «costituisce una forma di pedinamento eseguita con strumenti tecnologici, non assimilabile ad attività d'intercettazione prevista dall'art. 266 ss. c.p.c., ma piuttosto ad una attività di investigazione atipica i cui risultati sono senz'altro utilizzabili in sede di formazione del convincimento del giudice».

[25]Si veda, tra gli altri, A. Ingrao, *Il controllo a distanza effettuato mediante Social Network*, in "Labour & Law Issues", vol. 2, 2016, n. 1, p. 112.

[26]Si veda, ad esempio, Cass. civ., sez. lav., 18 febbraio 1983, n. 1236, in "Il Foro italiano", vol. 108, n. 7/8, pp. 2075-2076.

[27]Si veda Cass. pen., 8 ottobre 1985, in "Notiziario della giurisprudenza del lavoro", 1986, p. 155; Pret. Milano 4 ottobre 1988, in "Notiziario della giurisprudenza del lavoro", 1989, p. 436. In dottrina si veda, in proposito, C. Pisani, *Il computer e l'art. 4 dello Statuto dei lavoratori*, in R. De Luca Tamajo (a cura di), "Nuove tecnologie e tutela della riservatezza dei lavoratori", Milano, Franco Angeli, 1988, I ed., pp. 56 e 74.

[28]Secondo una diversa interpretazione, invece, alla distinzione terminologica fatta dal legislatore tra "installazione" e "impiego" degli strumenti di controllo non corrisponderebbe anche una diversificazione delle condizioni necessarie a legittimare l'una e l'altro, dovendosi ritenere che le finalità dell'impiego siano condizione anche per la legittima installazione dello strumento; in altri termini, non si considerano normativamente scindibili i due momenti della "installazione" e della "utilizzazione", per cui le condizioni necessarie alla legittimità di questa (presenza delle finalità aziendali) verrebbero comunque ad aggiungersi a quelle richieste per l'installazione (accordo o autorizzazione). Si veda in questo senso L. Alvino, *I nuovi limiti al controllo a distanza dell'attività dei lavoratori nell'intersezione fra le regole dello Statuto dei lavoratori e quelle del Codice della privacy*, in "Labour & Law Issues", vol. 2, 2016, n. 1, p. 15.

[29]Si vedano M. Marazza, *op. cit.*, p. 14; L. Tebano, *Tutela della privacy e potere di controllo del datore di lavoro tra l'ordinamento italiano e le fonti europee*, in "Labour & Law Issues", vol. 3, 2017, n. 2.

[30]In giurisprudenza, infatti, è da tempo riconosciuto il diritto al risarcimento dei danni derivanti dalle lesioni all'immagine dei soggetti giuridici. Sulla questione si veda Cass. 1° ottobre 2013, n. 22396, secondo cui nei confronti delle persone giuridiche e in genere degli enti collettivi è configurabile il risarcimento dei danni non patrimoniali se il fatto lesivo incide su situazioni giuridiche che siano equivalenti ai diritti fondamentali della persona umana costituzionalmente protetti, qual è il diritto all'immagine. La lesione deve essere tale da determinare una diminuzione della considerazione dell'ente o della persona giuridica da parte dei consociati in genere, ovvero di settori o categorie di essi, con cui i soggetti lesi di norma interagiscano. Per una pronuncia più recente si veda Cass., 16 novembre 2015, n. 23401.

[31]Si tratta del comunicato stampa fornito dal Ministero in data 2 febbraio 2018, in cui, sotto il titolo *Il Jobs Act non ha autorizzato i controlli a distanza dei lavoratori*, si dichiara esplicitamente che «con riferimento ad alcune osservazioni, riportate dalle agenzie di stampa, secondo le quali il Jobs Act avrebbe autorizzato l'utilizzo di dispositivi per il controllo a distanza dei lavoratori, si precisa che queste affermazioni non rispondono alla verità dei fatti».

[32]Si tratta, com'è noto, del "Codice in materia di protezione dei dati personali".

[33]Il Gruppo di studio "Articolo 29" (Working Party "Article 29") è il gruppo di lavoro europeo indipendente che ha trattato questioni relative alla protezione della vita privata e dei dati personali fino al 25 maggio 2018, data di entrata in vigore del Regolamento Generale per la Protezione dei Dati (General

Data Protection Regulation – GDPR) n. 2016/679. A decorrere da quella data il Gruppo "Articolo 29" è stato sostituito dal Comitato europeo per la protezione dei dati (European Data Protection Board – EDPB), organo incaricato di contribuire all'applicazione coerente delle norme sulla protezione dei dati e di promuovere la cooperazione tra le autorità competenti in tutta l'Unione Europea. È composto da rappresentanti delle autorità nazionali per la protezione dei dati e dal Garante europeo per la protezione dei dati (GEPD). Ne fanno però parte anche le autorità di controllo degli Stati della "European Free Trade Association" (EFTA) e della "European Economic Area" (EEA) per quanto riguarda le questioni connesse al GDPR, senza però che i loro rappresentanti abbiano il diritto di votare e di essere eletti presidente o vicepresidenti. Hanno, inoltre, diritto di partecipare, senza diritto di voto, alle attività e alle riunioni del Comitato, la Commissione europea e, con riferimento alle questioni connesse al regolamento generale sulla protezione dei dati, l'Autorità di vigilanza EFTA. Nell'ambito delle sue competenze l'EDPB può fornire orientamenti generali a chiarimento delle disposizioni normative e adottare decisioni vincolanti nei confronti delle autorità nazionali di controllo. In particolare, il 25 maggio 2018 l'EDPB ha approvato gli orientamenti relativi al regolamento generale sulla protezione dei dati, forniti dal precedente Gruppo di studio "Articolo 29".

[34]Si veda al riguardo la newsletter n. 430 del 24 luglio 2017 del Garante per la protezione dei dati personali.

[35]Nel documento citato nel testo – agevolmente accessibile, nella versione originale, ma anche tutte le lingue disponibili all'interno del sito europeo – sono integrate le precedenti pubblicazioni del gruppo di lavoro "Articolo 29" e cioè la *Opinion 8/2001 on the processing of personal data in the employment context (WP48)* e il *2002 Working Document on the surveillance of electronic communications in the worlplace (WP55)*.

[36]Si veda l'articolo *Privacy & lavoro, vietato "spiare" i social dei dipendenti*, in "Corriere Comunicazioni".

[37]Il Regolamento generale per la protezione dei dati personali costituisce la normativa di riforma della legislazione europea in materia di protezione dei dati. Pubblicato nella Gazzetta Ufficiale europea il 4 maggio 2016, è entrato in vigore il 24 dello stesso mese, ma la sua piena attuazione è avvenuta, a due anni di distanza, a decorrere dal 25 maggio 2018. Obiettivo del Regolamento è la definitiva armonizzazione della regolamentazione in materia di protezione dei dati personali all'interno dell'Unione europea. Trattandosi di un Regolamento, verrà attuato nello stesso modo in tutti i Paesi dell'Unione, senza margini di discrezionalità, non rendendosi necessario alcun atto di recepimento. L'art. 1, par. 2, inserisce esplicitamente il diritto alla protezione dei dati personali tra i diritti e le libertà fondamentali delle persone fisiche («Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali».).

[38]Il dibattito dottrinale sul tema è ormai molto vasto. Si vedano, tra gli altri: O. Dessì, *Il controllo a distanza sui lavoratori. Il nuovo art. 4 Stat. Lav.*, Napoli, ESI, 2017, 244 p.; E. Barraco, A. Sitzia, *Potere di controllo e privacy. Lavoro, riservatezza e nuove tecnologie*, Milano, IPSOA, 2016, XIII-331 p.; G. Fava, *Privacy e controllo dei lavoratori alla luce del Jobs Act*, Milano, Guerini Next, 2016, 251 p.; A. Levi, *Il controllo informatico sull'attività del lavoratore*, Torino, Giappichelli, 2013, 225 p.; P. Tullini (a cura di), *Tecnologie della comunicazione e riservatezza nel rapporto di lavoro. Uso dei mezzi elettronici, potere di controllo e trattamento dei dati personali*, Padova, Cedam, 2010, 194 p.; F. Bernabei, *Nuove tecnologie e tutela della riservatezza nei rapporti di lavoro*, Roma, LUMSA (Libera Università Maria Ss. Assunta), 2010, 193 p.

[39]Sul punto si veda ad esempio S. Petrilli, *Internet e posta elettronica sul luogo di lavoro: il garante ribadisce il divieto del controllo indiscriminato*, in "Azienditalia - Il personale", 2016, 575 p.

[40]Per alcune interessanti notazioni al riguardo, cfr. A. Sitzia, *Personal computer e controlli tecnologici del datore di lavoro nella giurisprudenza*, in "ADL - Argomenti di diritto del lavoro", 2017, n. 3, pp. 804-838.

[41]Al tema della rilevanza, sul rapporto di lavoro, dell'utilizzo extralavorativo dei social network è dedicato un distinto contributo su questo stesso numero della Rivista, cui si rinvia anche per ogni richiamo bibliografico in materia. Si veda F. Fameli, *La rilevanza giuridica dell'utilizzo extralavorativo dei social network da parte del lavoratore: utilizzabilità dei contenuti condivisi, obbligo di fedeltà e suo contemperamento col diritto di critica e con i diritti della persona costituzionalmente sanciti*, in questa *Rivista*, 2019, n. 1.

[42]Così recita l'art. 1, co. 7, lett. *f*), legge delega n. 183 del 2014.

[43]La vasta eco mediatica provocata dallo scandalo Facebook – Cambridge Analytica ha improvvisamente svelato le impressionanti dimensioni dei fenomeni collegati all'acquisizione delle enormi masse di dati che le nuove tecnologie consentono attualmente di registrare e trattare. In base alle notizie riportate dalle principali agenzie, le informazioni personali relative a ben 87 milioni di cittadini privati (non solo statunitensi, ma appartenenti anche a una decina di altre nazionalità, tra cui quella italiana) sarebbero state "impropriamente condivise" dalla società di consulenza utilizzata anche da Trump per la sua campagna elettorale. Per un aggiornamento sulle ripercussioni dello scandalo a livello mondiale, in vista anche dell'adeguamento al Regolamento europeo per la protezione dei dati, si veda G. Berruto, *F8, cosa aspettarsi dall'evento di Facebook*, 2018.

* * *

The labor law relevance of social networks, between workers protection and rights of control by the employers

Abstract: The introduction of computers and the use of social networks have led to a real revolution in the field of social relations and, in particular, in employment relationship. Obviously, the profiles involved are numerous, implying the emergence of new professional skills and the transformation of subordinate employment. In this context it is urgent to become aware of the fact that the breakthrough of new technologies in the world of work has made possible the creation and use of new, powerful and insidious forms of control of workers' activity. Article 23 of Legislative Decree no. 151/2015, issued by the Government in compliance with Law no. 183/2014, placing itself at the end of a long and storied path, has completely rewritten the Article 4 of the Workers' Statute, redefining the boundaries of the employer's control power,

also in relation to the use of the currently available technological tools. In this contribution, starting from the analysis of the jurisprudential elaboration and the doctrinal orientations in the matter of social networks and of remote controls on the activity of the workers, we highlight the main innovations introduced in the transition from the old to the new formulation of the statutory norm, having regarding also to the related problems of the worker's privacy protection.

Keywords: Workers activity – Control by the employer – Workers' privacy