Controlli difensivi

Controlli difensivi: quali i limiti nel nuovo contesto dell'art. 4, L. n. 300/1970

Cassazione Civile, Sez. I, 19 settembre 2016, n. 18302 - Pres. R. Bernabai - Est. Lamorgese - Istituto Poligrafico e Zecca dello Stato S.p.a. c. Garante per la protezione dei dati personali

Lavoro subordinato - Diritti ed obblighi del datore e del prestatore di lavoro - Libertà e dignità del lavoratore - In genere - Diritto alla riservatezza - Internet, posta elettronica, telefonia - Controlli difensivi - Limiti - Garanzie procedurali - Violazione degli artt. 4 e 8 della l. n. 300 del 1970 - Configurabilità

(Legge n. 300/1970, art. 4 e art. 8; D.Lgs. n. 196 /2003, art. 113)

In tema di tutela della riservatezza nello svolgimento del rapporto di lavoro, sono illegittime la conservazione e la categorizzazione dei dati personali dei dipendenti, relativi alla navigazione in internet, all'utilizzo della posta elettronica ed alle utenze telefoniche da essi chiamate, acquisiti dal datore di lavoro - benché affidatario, come nella specie, di compiti di rilievo pubblicistico - attraverso impianti e sistemi di controllo la cui installazione sia avvenuta senza il positivo esperimento delle procedure di cui all'art. 4, comma 2, L. n. 300 del 1970 (nel testo anteriore alle modifiche apportate dal D.Lgs. n. 151 del 2015), applicabili anche ai controlli diretti ad accertare comportamenti illeciti dei lavoratori quando comportino la possibilità di verifica a distanza dell'attività di questi ultimi, ed in assenza dell'acquisizione del consenso individuale e del rilascio delle informative previste dal D.Lgs. n. 196 del 2003. Il trattamento di quei dati si traduce, altresì, nella violazione dell'art. 8 della menzionata legge, che vieta lo svolgimento di indagini sulle opinioni e sulla vita personale del lavoratore, anche se le informazioni raccolte non siano in concreto utilizzate.

ORIENTAMENTI GIURISPRUDENZIALI	
Conforme	Cass. n. 22662/2016, v. anche Cass. Pen. 6 dicembre 2016, n. 51897.
Difforme	Cass. n. 19922/2016.

La Corte (*omissis*).

Considerato in diritto

Preliminarmente deve ricordarsi che il ricorrente ha domandato rimettersi la decisione del ricorso alle Sezioni Unite della Corte, in quanto occorre decidere su una questione di diritto già decisa in senso difforme dalla giurisprudenza di legittimità e perché trattasi di questione di massima di particolare importanza. Non si ritiene, però, di accogliere questa sollecitazione, perché la giurisprudenza di legittimità, dopo una pronuncia diretta in senso parzialmente contrario, ha poi adottato una linea interpretativa evolutiva e coerente, cui il Collegio ritiene di dare continuità.

1. Con il primo motivo di impugnazione (in cui possono esaminarsi congiuntamente i motivi indicati come I, Ia, Ib e II), l'Istituto Poligrafico e Zecca dello Stato ha dedotto, ai sensi dell'art. 360 c.p.c., n. 3, la violazione e falsa applicazione della L. n. 300 del 1970, artt. 4 e 8, (Statuto dei lavoratori), e degli artt. 12 e 14 preleggi, nonché art. 11, comma 1, lett. a), c) e d), e artt. 113 e 114 Codice Privacy (D.Lgs. n. 196 del 2003), per avere il Tribunale di Roma ritenuto applicabile alla fattispecie l'art. 4 cit., secondo comma, e non operativa la categoria dei controlli difensivi.

Secondo il ricorrente, l'art. 4 "non esaurisce tutte le ipotesi di controllo del datore di lavoro sulla condotta tenuta dal lavoratore in azienda intesa nella sua ampiezza, per la semplicissima ragione che quella norma regolamenta solo il profilo attinente il controllo sull'attività lavorativa... rimangono completamente fuori dal confine operativo della norma i controlli che abbiano ad oggetto non l'attività lavorativa, ma altri comportamenti tenuti dal lavoratore sul posto di lavoro, e segnatamente quelli illeciti, che espongano ad un pericolo i beni dell'azienda e/o concretino fatti potenzialmente dannosi

per i terzi, con conseguente responsabilità del datore di lavoro".
Trattasi di esigenza che assumerebbe in questo caso un particolare rilievo, in considerazione delle attribuzioni di interesse pubblicistico assegnate all'Istituto Poligrafico, come la stampa della Gazzetta Ufficiale e della Raccolta ufficiale degli atti normativi della Repubblica italiana, la produzione di documenti identificativi della persona, di sistemi di sicurezza e anticontraffazione, di monete, ecc. Nella prospettazione del ricorrente, "il tratto distintivo dell'art. 4, tanto al comma 1 quanto al comma 2, è ravvisabile nell'aver circoscritto il proprio campo di applicazione solo ed esclusivamente al controllo sull'attività lavorativa dei dipendenti". Nel caso di specie, i controlli predisposti dal Poligrafico non atterrebbero alle esigenze organizzative e produttive ovvero alla sicurezza del lavoro, di cui all'art. 4, comma 2, dello Statuto dei lavoratori, bensì ad esigenze di "tutela del patrimonio aziendale".
Con riferimento alla navigazione in Internet da parte dei dipendenti, l'utilizzazione del sistema Websense era stata prevista proprio per la finalità di rispettare le esigenze di prevenzione volte a ridurre il rischio di utilizzazioni improprie della navigazione, ed è per questo che il sistema assicurava che determinati siti fossero inaccessibili dalla rete aziendale. Il Tribunale erroneamente aveva condiviso le censure del Garante, in materia di conservazione dei dati relativi alla navigazione in Internet di ciascun dipendente, mentre i dati venivano conservati per finalità di tutela aziendale e per potere, se del caso, informare l'Autorità Giudiziaria di eventuali illeciti. Inoltre, la navigazione in Internet, se non controllata, comporterebbe la possibilità di rischi (come la possibilità di acquisire virus nella rete aziendale) che un'azienda con le attribuzioni pubblicistiche proprie del Poligrafico non può consentire.
In ogni caso, l'art. 8 dello Statuto dei lavoratori vieta la "effettuazione" attiva delle indagini sulle opinioni politiche, religiose o sindacali dei dipendenti e non già la mera possibilità di effettuazione delle medesime.
Quanto alla presunta violazione dell'art. 11 del Codice Privacy e del principio di pertinenza e non eccedenza dei controlli, se non vi fosse la possibilità di acquisire e conservare i dati identificativi dei contatti Internet (utente che richiede il contatto, sito contattato o che si tenta di contattare, data ed ora dell'accesso o del tentativo), sarebbe preclusa la tutela delle ragioni di sicurezza, sicché anche questa materia dovrebbe essere ricondotta nell'alveo dei cd. controlli difensivi.
1.1 Il motivo è infondato.
È opportuno premettere che il rilievo pubblicistico dei compiti affidati all'Istituto Poligrafico dello Stato non è idoneo a giustificare la violazione della normativa vigente, che intende assicurare garanzia ai diritti costituzionalmente riconosciuti ai lavoratori, in primo luogo al diritto alla riservatezza.
Il ricorrente afferma, in sostanza, che spetta al datore di lavoro predisporre tutti gli strumenti necessari per la tutela dei beni aziendali rispetto a possibili danni ed accertare e prevenire comportamenti illeciti dei dipendenti, purché non abbiano quale scopo diretto la vigilanza sulla prestazione di lavoro fornita dai dipendenti (L. n. 300 del 1970, art. 4, comma 1) e non siano finalizzati alla tutela di esigenze organizzative e produttive, ovvero della sicurezza del lavoro (art. 4, comma 2, legge cit.).
È necessario esaminare l'art. 4 dello Statuto dei Lavoratori.
Esso prevede, al comma 1, il divieto assoluto per il datore di lavoro di utilizzare "impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori", ma non è questa la contestazione rivolta all'Istituto Poligrafico, non risultando che i controlli sulla navigazione in Internet e sull'utilizzo dei servizi di telefonia e posta elettronica siano stati specificamente predisposti per finalità di vigilanza a distanza dell'attività lavorativa dei dipendenti.
Il secondo comma prevede che "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, possono essere istallati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti". Nel giudizio in esame è pacifico che il ricorrente Istituto Poligrafico non ha mai ricercato un accordo con le rappresentanze dei lavoratori al fine di disciplinare i controlli, e neppure ha promosso le procedure suppletive che la legge prevede siano svolte qualora un accordo non sia raggiunto.
Si deve operare, in materia, un contemperamento tra i diritti del datore di lavoro e, in particolare, alla libera iniziativa economica ed alla protezione dei beni aziendali, con la tutela del diritto del lavoratore, in primo luogo alla riservatezza. Questo bilanciamento non è affidato alla valutazione della giurisprudenza, avendo il legislatore provveduto a dettare la disciplina generale della materia, in primo luogo proprio mediante le norme previste dall'art. 4 dello Statuto dei lavoratori. Per comprenderne l'esatta portata, è necessario esaminare, oltre il suo testo letterale, anche la finalità della norma.
La disposizione di cui all'art. 4, comma 2, in esame collocata nel Titolo I dello Statuto, che prescrive regole per la tutela della libertà e dignità del lavoratore è rivolta ad assicurare al lavoratore che il controllo a distanza, anche solo potenziale, della sua attività lavorativa sia protetto da garanzie, qualunque sia la finalità per la quale il datore di lavoro predispone i controlli. Quando l'attività di vigilanza a distanza, attivata dal datore di lavoro per qualsiasi finalità, permetta anche la mera "possibilità di controllo dell'attività lavorativa" fornita dal prestatore di lavoro, l'attività non è consentita se non a seguito del positivo esperimento delle procedure di garanzia di cui all'art. 4, comma 2, del medesimo Statuto. Non è possibile ritenere che il datore di lavoro possa liberamente utilizzare impianti e apparecchiature di controllo per qualsiasi finalità (di

tutela dei beni aziendali, di accertamento e prevenzione dei comportamenti illeciti dei dipendenti, ecc.), eludendo il positivo esperimento delle procedure previste nell'art. 4, comma 2, in esame, quando derivi anche solo "la possibilità di controllo a distanza dell'attività dei lavoratori", a prescindere dalle sue intenzioni.
Questa conclusione non si pone in contrasto con l'evoluzione della giurisprudenza di legittimità in materia.
È vero che una risalente decisione della Suprema Corte aveva affermato che il controllo diretto ad accertare condotte illecite del lavoratore, cd. controllo difensivo, non sarebbe assoggettato alla disciplina di cui all'art. 4 dello Statuto dei lavoratori (Cass., Sez. L., n. 4746 del 2002). Questo orientamento ha ricevuto però smentita da una successiva pronuncia di questa Corte, la quale ha precisato che "la garanzia procedurale prevista per impianti ed apparecchiature ricollegabili ad esigenze produttive contempera l'esigenza di tutela del diritto dei lavoratori a non essere controllati a distanza e quello del datore di lavoro o, se si vuole, della stessa collettività, relativamente alla organizzazione, produzione e sicurezza del lavoro, individuando una precisa procedura esecutiva e gli stessi soggetti ad essa partecipi"; ha quindi chiarito che l'utilizzo di un'apparecchiatura comunque idonea ad esercitare la vigilanza a distanza sui prestatori di lavoro, si risolve "in un controllo... rientrante nella fattispecie prevista dalla L. n. 300 del 1970, art. 4, comma 2, né l'esigenza di evitare condotte illecite da parte dei dipendenti può assumere portata tale da giustificare un sostanziale annullamento di ogni forma di garanzia della dignità e riservatezza del lavoratore" (Cass. Sez. L, n. 15892 del 2007).
La suddetta linea interpretativa, contrariamente a quanto affermato dal ricorrente, ha ricevuto molteplici conferme nella giurisprudenza di questa Corte. Ad esempio, in un caso in cui il datore di lavoro utilizzava programmi informatici che consentivano il monitoraggio della posta elettronica e degli accessi Internet dei dipendenti, il Giudice di legittimità ha ritenuto applicabili le "garanzie procedurali imposte dalla L. n. 300 del 1970, art. 4, comma 2, per l'istallazione di impianti ed apparecchiature di controllo dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori", dopo avere evidenziato la necessità di contemperare le esigenze del datore di lavoro con i diritti del prestatore di lavoro; pertanto, anche i controlli cd. difensivi "diretti ad accertare comportamenti illeciti dei lavoratori", quando comportino la possibilità del controllo a distanza della prestazione lavorativa dei dipendenti, sono soggetti alla disciplina di cui all'art. 4, comma 2, dello Statuto dei lavoratori (v. Cass., Sez. L, n. 4375 del 2010, n. 16622 del 2012, le quali affermano che "la possibilità di effettuare tali controlli incontra un limite nel diritto alla riservatezza del dipendente, tanto che anche l'esigenza di evitare condotte illecite dei dipendenti non può assumere portata tale da giustificare un sostanziale annullamento di ogni forma di garanzia della dignità e riservatezza del lavoratore").
Di recente, questa Corte ha confermato che un'apparecchiatura predisposta dal datore di lavoro ("badge" idoneo a controllare l'ingresso e l'uscita del dipendente, ma anche le pause ed i permessi, ed a comparare nell'immediatezza i dati di tutti i dipendenti) "ove sia utilizzabile anche in funzione di controllo a distanza del rispetto dell'orario di lavoro e della correttezza dell'esecuzione della prestazione... è illegittima, ai sensi della L. n. 300 del 1970, art. 4, comma 2, se non concordata con le rappresentanze sindacali, ovvero autorizzata dall'Ispettorato del lavoro, dovendosi escludere che l'esigenza di evitare condotte illecite da parte dei dipendenti possa assumere portata tale da giustificare un sostanziale annullamento di ogni forma di garanzia della dignità e riservatezza del lavoratore" (Cass., Sez. L, n. 9904 del 2016).
Corretta è anche la contestazione del Garante, confermata dal Tribunale, relativa alla violazione del disposto di cui all'art. 8 dello Statuto dei lavoratori. La norma prevede che è vietato al datore di lavoro "effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore". Ed acquisire e conservare dati che contengono (o possono contenere) simili informazioni importa già l'integrazione della condotta vietata, perché si risolve in una indagine non consentita sulle opinioni e condotte del lavoratore, anche se i dati non sono successivamente utilizzati.
Non è necessario sottoporre i dati raccolti ad alcun particolare trattamento per incorrere nell'illecito, poiché la mera acquisizione e conservazione della disponibilità di essi comporta la violazione della prescrizione legislativa.
Il motivo deve essere, pertanto, disatteso.
2. Con il secondo motivo (nn. IIa, IIb), l'Istituto ricorrente ha denunciato, ai sensi dell'art. 360 c.p.c., n. 3, la violazione o falsa applicazione dell'art. 4 dello Statuto dei lavoratori e degli artt. 12 e 14 preleggi, perché la natura di controllo difensivo dell'attività posta in essere escluderebbe l'applicabilità della normativa indicata. Inoltre, è contestato, ai sensi dell'art. 360 c.p.c., n. 5, l'omesso esame di un fatto decisivo per il giudizio, costituente oggetto di discussione tra le parti, per non avere il Tribunale pronunciato sulle modalità di utilizzo dei dati raccolti mediate il software Websense con finalità esclusiva di controllo difensivo.
Il ricorrente ha confermato di avere inibito ai dipendenti l'accesso a determinati siti Internet considerati pericolosi e provveduto alla registrazione dei cd. file Log (identificativi di indirizzo Ip, cioè della postazione di lavoro, dell'utenza contattata, della data ed ora dell'accesso o del tentativo di accesso), ma ha affermato che si tratta di un'attività svolta per esclusiva finalità di tutela aziendale. Si dovrebbe tenere conto che i lavoratori erano stati resi edotti del fatto che i file di log venivano registrati con questa finalità, che la mancata registrazione precluderebbe la prevenzione ed esporrebbe l'Istituto ad attacchi non identificabili alla rete aziendale. In ogni caso, non sarebbe configurabile alcuna viola-

zione dell'art. 8 dello Statuto dei lavoratori, che vieta la "effettuazione" attiva delle indagini sulle opinioni politiche, religiose o sindacali dei dipendenti, e non la mera possibilità di effettuazione delle medesime, non avendo l'Istituto mai effettuato alcuna indagine sui profili extraprofessionali dei lavoratori.
2.1 Il motivo è inammissibile nella parte in cui denuncia, da un lato, una insufficienza motivazionale che non è più censurabile, a norma del novellato art. 360 c.p.c., n. 5 (v. Cass., Sez. Un., n. 8053 del 2014) e, dall'altro, la prevalenza attribuita dal Giudice di merito, nel percorso motivazionale, ad alcune circostanze piuttosto che ad altre, implicitamente respinte, le quali sono prive del carattere della decisività, nel senso che una diversa valutazione delle stesse non avrebbe determinato un esito diverso della decisione.
Infatti, si è già argomentato in ordine all'obbligo di portare positivamente a compimento le procedure di cui all'art. 4, secondo comma, dello Statuto dei lavoratori, quando l'attività di vigilanza sia anche solo potenzialmente idonea a comportare il controllo dell'attività svolta dai lavoratori.
Nel giudizio di merito si è accertato che il Poligrafico provvedeva - non solo alla, di per sé lecita, inibizione dell'accesso dei lavoratori a determinate categorie di siti Internet, ma anche - alla registrazione dei cd. file Log (identificativi di indirizzo Ip, cioè della postazione di lavoro, dell'utenza contattata, della data ed ora dell'accesso o del tentativo di accesso), senza che fossero state espletate le procedure previste dalla legge per lo svolgimento delle attività che comportino anche solo la possibilità di controllo a distanza dei lavoratori. Ed è irrilevante che i lavoratori fossero stati messi a conoscenza delle modalità di acquisizione dei dati di traffico, conservati per un periodo di tempo prolungato (da sei mesi a un anno).
Inoltre, la acquisizione e conservazione dei dati relativi alla navigazione Internet dei dipendenti mediante captazione e registrazione dei file Log importa la violazione anche del disposto di cui alla L. n. 300 del 1970, art. 8, per le ragioni innanzi indicate (v., supra, 1.1, in fine).
Il motivo è rigettato.
3. Con il terzo motivo di ricorso (nn. IIIa, IIIb), in riferimento alla gestione del servizio di posta elettronica, il Poligrafico ha contestato, ai sensi dell'art. 360 c.p.c., n. 3, la violazione o falsa applicazione degli artt. 2 e 13 del Codice della Privacy, per avere il Tribunale censurato la condotta del Poligrafico per non avere fornito ai lavoratori una informazione adeguata sulle modalità di trattamento dei dati, in relazione alla conservazione di quelli relativi alle comunicazioni in chiaro, e limitatamente ai lavoratori che avessero deciso di avvalersi del server aziendale per la conservazione dei messaggi di posta elettronica. Si assume che tale informazione non fosse prevista dalle citate norme, ma eventualmente dalle Linee Guida sulla Posta Elettronica ed Internet, emanate dal Garante il 1 marzo 2007, disciplina la cui violazione (cfr. art. 154, comma 1, lett. c, del Codice della Privacy) non era stata contestata al ricorrente. Inoltre, sempre con riferimento al servizio di posta elettronica, è denunciato, ai sensi dell'art. 360 c.p.c., comma 5, l'omesso esame circa un fatto decisivo per il giudizio, costituente oggetto di discussione tra le parti, per non avere il Tribunale pronunciato in ordine alla completezza dell'informazione assicurata dal Poligrafico ai propri dipendenti. È stato evidenziato che ad ogni singolo utente era lasciata la facoltà di far conservare i messaggi e-mail sulla mailbox aziendale e che ciò attestava come i dipendenti fossero ben informati e consapevoli del fatto che la scelta effettuata comportava che i messaggi rimanevano conservati anche sul server ed erano accessibili agli amministratori del sistema; che era attivo un servizio di help-desk per la configurazione del servizio di posta elettronica, a disposizione dei lavoratori, i quali potevano ricevere idonee informazioni circa le possibili modalità di configurazione del servizio; che dal documento PR-FSIA2-209, che si afferma essere stato distribuito al personale, erano ricavabili "indicazioni" che consentivano di apprendere che la Unità Organizzativa Gestione Sistemi dell'Area ICT e Business Solutions avrebbe potuto accedere alle risorse informatiche dell'utente, ai fini di sicurezza del sistema; infine, sulla rete intranet aziendale, consultabile da qualsiasi dipendente, sin dal marzo 2010, erano indicati gli identificativi degli amministratori di sistema abilitati ad accedere ai dati raccolti nel sistema informatico del Poligrafico.
3.1 Il Giudice di merito ha reso una motivazione, pienamente adesiva alle argomentazioni del Garante, adeguata e non censurabile sotto il profilo della insufficienza (a norma del nuovo art. 360 c.p.c., n. 5), in ordine alla illiceità del trattamento relativo ai servizi di posta elettronica. Il ricorrente deduce, in questa sede, varie circostanze di fatto - ritenute implicitamente irrilevanti dal Giudice di merito - e chiede impropriamente al Giudice di legittimità di esaminarle, senza neppure spiegare se e in quale atto siano state fatte valere nel giudizio di merito.
Si obietta che a tutti i lavoratori erano state fornite informazioni specifiche, idonee a soddisfare le prescrizioni di cui all'art. 13 del Codice della Privacy, mediante la consegna di documenti non prodotti, però, nella fase ispettiva e il cui contenuto non è stato trascritto nel ricorso.
Inoltre, il fatto di aver fornito informazioni ai propri dipendenti non è elemento decisivo per escludere la violazione del disposto di cui all'art. 4, comma 2, dello Statuto dei lavoratori.
Deve aggiungersi che quand'anche si informino i lavoratori della possibilità di archiviare i messaggi di posta elettronica sul server aziendale oppure sul PC messo a disposizione dall'azienda, questo non comporta che essi siano resi edotti che, scegliendo la prima opzione, i loro messaggi rimarranno, per un periodo di tempo prolungato, accessibili in chiaro dai soggetti abilitati alla consultazione.
Il motivo è rigettato.
4. Con il quarto motivo (nn. IVa e IVb), il ricorrente ha contestato, ai sensi dell'art. 360 c.p.c., n. 3, la viola-

zione e falsa applicazione dell'art. 4 dello Statuto dei lavoratori e degli artt. 12 e 14 preleggi, nonché, ai sensi dell'art. 360 c.p.c., n. 5, l'omesso esame circa un fatto decisivo per il giudizio, costituente oggetto di discussione tra le parti, in relazione all'esercizio del servizio di telefonia.
Si assume che il Tribunale abbia omesso di pronunciare sulle argomentazioni dell'Istituto Poligrafico, di seguito riportate.
Il servizio di telefonia, cd. sistema VoIP, veniva gestito mediante l'applicativo Bluès, grazie al quale il Poligrafico aveva accesso ai dati raccolti e conservati dal sistema, configurato in modo da rilevare eventuali telefonate ingiustificate effettuate dalle utenze assegnate ai dipendenti; i numeri chiamanti assegnati ai dipendenti non venivano registrati, mentre i numeri chiamati venivano esterne; i dati di traffico erano conservati "per di 180 giorni", per esigenze di documentazione in contestazione della fatturazione da parte delle esterne; pur essendo disponibile nell'applicativo Bluès la funzione "alert", che consentiva l'invio, ad un indirizzo di posta elettronica prescelto dal datore di lavoro, di un messaggio di avviso ogni qual volta il sistema avesse rilevato una chiamata telefonica verso numeri esterni preindicati come da monitorare, la stessa funzione non era stata mai attivata.
4.1 Il motivo è infondato.
Si deve rilevare che l'affermazione del ricorrente, secondo cui i numeri del traffico telefonico relativo ai dipendenti non erano conservati e che, nel conservare documentazione dei numeri telefonici chiamati dai propri dipendenti, ne fossero occultate le ultime tre cifre, è smentita dalle risultanze processuali. Il Giudice di merito dà atto del contrario: sarebbe stato preciso onere della parte indicare specificamente su quale atto processuale la sua affermazione potesse trovare fondamento.
Non è pertinente l'obiezione secondo la quale la prolungata conservazione dei dati relativi al traffico sarebbe stata prevista solo per il caso di eventuali contestazioni della fatturazione da parte dei soggetti terzi: non si vede, infatti, in qual modo il soddisfacimento di questa esigenza dovesse comportare la conservazione dei dati relativi al traffico telefonico anche dei dipendenti e per un prolungato periodo di tempo.
In ordine alla funzione "alert", prevista dall'applicativo Bluès, il Giudice di merito, implicitamente e plausibilmente, l'ha ritenuta lesiva dei diritti dei lavoratori, in assenza del positivo espletamento delle procedure di cui all'art. 4, comma 2, dello Statuto dei lavoratori, ed è corretta, pertanto, la richiesta del Garante di escluderla, a prescindere dal fatto che essa fosse stata concretamente utilizzata.
Si deve dare continuità all'orientamento espresso da questa Corte a proposito del controllo del traffico telefonico dei dipendenti, attuato mediante il sistema Bluès, che si sosteneva essere giustificato (anche) per esigenze di contrasto alle attività illecite che avrebbero potuto essere poste in essere dai lavoratori a danno del datore di lavoro e, quindi, estraneo all'ambito applicativo della L. n. 300 del 1970, art. 4, trattandosi asseritamente di una modalità di controllo difensivo lecito. A queste obiezioni la Cassazione ha replicato, affermando che " l'effettività del divieto di controllo a distanza dell'attività dei lavoratori richiede che anche per i cd. controlli difensivi trovino applicazione le garanzie del citato art. 4, comma 2, e che, comunque, quest'ultimi, così come la altre fattispecie di controllo ivi previste, non si traducano in forme surrettizie di controllo a distanza dell'attività lavorativa dei lavoratori. Se per l'esigenza di evitare attività illecite o per motivi organizzativi o produttivi, possono essere installati impianti ed apparecchiature di controllo che rilevino dati relativi anche alla attività lavorativa dei lavoratori, la previsione che siano osservate le garanzie procedurali di cui all'art. 4, comma 2, non consente che attraverso tali strumenti, sia pure adottati in esito alla concertazione con le r.s.a., si possa porre in essere, anche se quale conseguenza mediata, un controllo a distanza dei lavoratori che, giova ribadirlo, è vietato dall'art. 4, comma 1, cit. Il divieto di controlli a distanza L. n. 300 del 1970, ex art. 4, implica, dunque, che i controlli difensivi posti in essere con il sistema informatico Bluès 2002, ricadono nell'ambito della L. n. 300 del 1970, art. 4, comma 2" (Cass. Sez. L, n. 16622 del 2012 cit.).
5. Con il quinto motivo (n. Va) è contestato, ai sensi dell'art. 360 c.p.c., n. 5, l'omesso esame di un fatto decisivo per il giudizio, costituente oggetto di discussione tra le parti, in quanto - contrariamente a quanto contestato dal Garante - il Poligrafico aveva provveduto a rendere conoscibile l'identità degli amministratori di sistema.
5.1 Il motivo è infondato.
Il Giudice di merito ha plausibilmente ritenuto, in senso adesivo alle argomentazioni del Garante, che il Poligrafico, in violazione dell'art. 4, comma 2, dello Statuto dei lavoratori, aveva utilizzato strumenti elettronici che consentivano la vigilanza a distanza dei dipendenti, senza che fossero state espletate le procedure previste dalla legge. A fronte di tale accertamento, è irrilevante la circostanza che i lavoratori fossero stati portati a conoscenza dei nominativi degli amministratori abilitati ad accedere al sistema informatico aziendale.
6. In conclusione, il ricorso è rigettato.
Le spese di lite, liquidate in dispositivo, seguono la soccombenza.
(*omissis*).

IL COMMENTO

di Paola Salazar e Luca Failla (*)

L'innovazione tecnologica guida l'evoluzione del diritto, ma la giurisprudenza procede spesso con più lentezza. L'interpretazione che per anni è stata proposta dalla giurisprudenza in materia di controlli a distanza, che ha aperto la strada al progressivo riconoscimento dei "controlli difensivi", continuerà ad avere influenza sulla interpretazione e applicazione pratica del nuovo art. 4 della L. n. 300/1970. I giudici della suprema Corte di cassazione hanno sì iniziato ad inserire nel proprio orientamento valutazioni che appaiono il frutto del rinnovato contesto normativo e dell'opera di "attualizzazione" della norma voluti dal legislatore con il Jobs Act. Ma stanno altresì svolgendo un'opera di riadattamento di principi elaborati in applicazione della vecchia norma, al nuovo contesto della moderna organizzazione del lavoro.
È presumibile che nel quadro del novellato art. 4 dello Statuto dei lavoratori il discrimine tra liceità e illiceità nell'eventuale uso a fini disciplinari dei dati raccolti attraverso gli strumenti di lavoro, sarà costituito - nel quadro di nuove e più rigorose policy interne - dalla valutazione in merito alla sua indispensabilità nel rendere la prestazione lavorativa e dalla effettività della procedura seguita per la sua istallazione e per il suo uso.

Premessa

L'innovazione tecnologica guida l'evoluzione del diritto. È quello che è in pratica avvenuto in questi ultimi venti/trenta anni nell'applicazione pratica dello Statuto dei lavoratori, soprattutto in materia di videosorveglianza e di controlli a distanza, fino ad arrivare alla revisione delle disposizioni dell'art. 4, L. n. 300/1970 - riformato dall'art. 23 del D.Lgs. n. 151/2015 - ed è quello che dovremo attenderci nell'evoluzione giurisprudenziale di questa materia, grazie anche agli spazi di manovra aperti dalla nuova disciplina introdotta dal *Jobs Act*, anche se questo processo si prospetta piuttosto lento e in salita.
L'interpretazione che per anni è stata proposta dalla giurisprudenza in questa materia, in applicazione del vecchio testo dell'art. 4 dello Statuto dei lavoratori, si è attestata in modo praticamente univoco, come noto, sulla nota contrapposizione tra divieto "assoluto" e divieto "relativo" di controllo così come proposti, rispettivamente, dal primo e dal secondo comma della norma - nel testo previgente le modifiche apportate dall'art. 23 del D.Lgs. n. 151/2015. Tale prospettazione che ha di fatto aperto la strada al riconoscimento da parte della giurisprudenza dei "controlli difensivi" (1) - si ritiene che possa svolgere un ruolo primario ancora per molti anni in questa materia se, come è possibile constatare dalla giurisprudenza degli ultimi mesi, la Cassazione ritiene di riaffermare con forza alcuni fondamentali principi.
Si tratta, in pratica, di una serie di criteri guida che seppure attenuati nel nuovo testo normativo, permangono tuttavia come presupposto fondante la generale ammissibilità del controllo in materia di lavoro. Principi che hanno costituito per anni la base per gli interventi del Garante della Privacy in materia e che continuano a guidare anche oggi lo stesso Garante - come si dirà - e, presumibilmente, anche la Cassazione. I supremi giudici sono infatti intervenuti nell'ultimo anno a valutare situazioni giuridiche che, seppure formatesi nel vigore della vecchia disciplina, stanno creando lo sfondo per quella che presumibilmente potrà essere l'evoluzione giurisprudenziale che deriverà dall'applicazione della norma nel testo novellato.
I giudici della suprema Corte di cassazione hanno di fatto iniziato ad inserire nel proprio orientamento valutazioni che appaiono il frutto - necessariamente - del rinnovato contesto normativo e dell'opera di "attualizzazione" della norma voluta dal legislatore con il Jobs Act. Quasi a voler sottolineare da un lato che il rinnovamento voluto dal legislatore in questa materia non è altro che la necessaria traduzione in legge di principi che la giurisprudenza stava già da anni elaborando. Ma hanno ritenuto di riaffermare, dall'altro che tali principi, nella

(*) N.d.R.: Il presente contributo è stato sottoposto, in forma anonima, al vaglio del Comitato di valutazione.

(1) Per un riepilogo dell'evoluzione avuta dalla materia, in dottrina cfr. P. Lambertucci, *Il controllo del datore di lavoro e tutela della privacy*, in G. Santoro Passarelli (a cura di), *Diritto e processo del lavoro e della previdenza sociale*, Milano, 2014; M. Miscione, *I controlli intenzionali, preterintenzionali e difensivi sui lavoratori in contenzioso continuo*, in questa *Rivista*, 2013, 8/9, 761.

loro portata generale, non verranno - o non vorranno essere - per nulla alterati dall'applicazione pratica delle nuove disposizioni, soprattutto alla luce delle implicazioni pratiche - anche penali - derivanti dall'uso delle nuove tecnologie.
Vediamo come.

I limiti del controllo nell'uso di specifici software

Innanzitutto, continua ad emergere con particolare vigore che le modalità di controllo attuate con strumenti informatici non possono quasi mai rientrare tra i controlli "difensivi" ammessi dalla norma per le finalità connesse con esigenze organizzative ovvero di tutela del patrimonio aziendale o per ragioni di sicurezza. Cass., Sez. lav., 9 settembre 2016, n. 18302 - qui in commento - afferma in buona sostanza che se per l'esigenza di evitare attività illecite o per motivi organizzativi o produttivi, possono essere installati impianti ed apparecchiature di controllo dai quali possano essere ricavati anche dati relativi all'attività lavorativa dei lavoratori, è tuttavia possibile utilizzare tali dati solo in presenza delle garanzie derivanti dall'accordo sindacale o dalla procedura di autorizzazione amministrativa. In mancanza, si realizza in ogni caso una forma di controllo a distanza, vietato, perché lesivo della dignità del lavoratore, in violazione delle disposizioni dell'art. 8, L. n. 300/1970. Ciò coerentemente - peraltro - con gli orientamenti espressi in questi anni dal Garante della Privacy, sempre molto restrittivi, soprattutto alla luce delle potenzialità di controllo occulto derivanti dai nuovi strumenti tecnologici.
Ora, seppure il principio viene affermato con riguardo al contenuto della vecchia norma, spicca tuttavia il ragionamento usato dai supremi giudici nella valutazione della utilizzabilità di uno strumento necessario a limitare il più possibile la commissione di illeciti. Nel caso specifico si trattava di un software finalizzato - nell'interesse del datore di lavoro (Poligrafico e Zecca dello Stato S.p.A) - a limitare la navigazione internet ma dal quale potevano essere ricavati anche dati relativi allo svolgimento dell'attività lavorativa.
La Corte nel confermare il divieto - in senso assoluto - posto dalla norma di cui all'art. 4 (vecchio testo) ha di fatto recuperato orientamenti già espressi ad esempio con riguardo al badge elettronico (cfr. Cass., Sez. lav., n. 9904/2016) così come al controllo del traffico telefonico (cfr. Cass., Sez. lav., n. 16622/2012) statuendo che la norma non consente mai che attraverso tali strumenti - sia pure adottati in esito alla concertazione con le rappresentanze sindacali o attraverso provvedimento amministrativo - si possa porre in essere, anche solo quale conseguenza mediata, un controllo a distanza dei lavoratori.
In senso conforme statuisce Cass., Sez. lav., 8 novembre 2016, n. 22662 che spicca in particolare per le implicazioni che potrà avere lo sviluppo della futura giurisprudenza in questa materia. Si afferma infatti che: "l'art. 4 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 che la vigilanza sul lavoro, ancorché necessaria all'organizzazione produttiva vada mantenuta in una dimensione umana e cioè non esasperata dall'uso di tecnologie che possono rendere la vigilanza stessa continua ed anelastica, eleminando ogni zona di riservatezza e di autonomia nello svolgimento del lavoro - (Cass. n. 15892/2007 e Cass. n. 2722/2012) -. La tutela del diritto alla riservatezza non consente di escludere che rientrino nella fattispecie di cui al citato art. 4 i controlli diretti ad accertare comportamenti illeciti dei lavoratori nel caso in cui la sorveglianza riguardi l'espletamento dell'attività lavorativa e venga attuata mediante strumenti potenzialmente lesivi della sfera personale, la cui utilizzazione è subordinata al previo accordo con il sindacato o all'intervento dell'Ispettorato del lavoro." A parere della Corte il controllo preterintenzionale che può generarsi grazie all'uso delle più moderne tecnologie risulterebbe così sempre vietato.
Dello stesso avviso la più recente decisione della Cass. Pen. 6 dicembre 2016, n. 51897 la quale afferma che "con la rimodulazione dell'art. 4 dello Statuto dei lavoratori, è solo apparentemente venuto meno il divieto esplicito di controlli a distanza, nel senso che il superamento del divieto generale di detto controllo non può essere predicato sulla base della mancanza nel nuovo art. 4, di una indicazione espressa (com'era al comma 1 del previgente art. 4) di un divieto generale di controllo a distanza sull'attività del lavoratore, avendo la nuova formulazione *solamente adeguato l'impianto normativo* alle sopravvenute innovazioni tecnologiche e, quindi, mantenuto fermo il divieto di controllare la sola prestazione lavorativa dei dipendenti, posto che l'uso di impianti audiovisivi e di altri strumenti di controllo può essere giustificato 'esclusivamente'

a determinati fini, che sono '*numerus clausus*'(cioè per esigenze organizzative e produttive; per la sicurezza del lavoro e per la tutela del patrimonio aziendale) e alle condizioni normativamente indicate, sicché residua un regime protezionistico diretto a salvaguardare la dignità e la riservatezza dei lavoratori, la cui tutela rimane primaria nell'assetto ordinamentale e costituzionale seppur bilanciabile sotto il profilo degli interessi giuridicamente rilevanti con le esigenze produttive ed organizzative o della sicurezza sul lavoro" (2).

La posizione del Garante: nel segno della continuità?

Tenendo conto dello sviluppo che la giurisprudenza ha avuto negli ultimi anni, soprattutto alla luce dell'influenza che il progresso tecnologico ha esercitato nella valutazione dei limiti nell'uso degli strumenti di lavoro e degli orientamenti espressi da ultimo dalla suprema Corte di cassazione, vi è da ipotizzare che tale orientamento mantenga validità per una parte (o gran parte) della giurisprudenza anche nel nuovo contesto della norma scaturita dal Jobs Act. E ciò forse grazie anche al richiamo espresso alla tutela della privacy contenuto oggi nella norma novellata e, sulla base di questo, per effetto degli orientamenti - invero molto restrittivi - espressi dal Garante della Privacy negli ultimi mesi proprio in forza delle novità contenute nel vigente art. 4, L. n. 300/1970.
Si fa riferimento, in particolare, al provvedimento n. 303 del 13 luglio 2016 e al provvedimento n. 350 dell'8 settembre 2016. Nel primo caso il Garante ha vietato l'uso dei sistemi di tracciamento della navigazione internet di un Ateneo sulla base della possibilità che attraverso il MAC Address (Media Access Control Address), della "interfaccia" di rete di una postazione si potesse di fatto risalire comunque ad uno specifico dispositivo di rete e da questo all'identità del produttore, alla tipologia di dispositivo e, in taluni casi, anche risalire all'acquirente o utilizzatore dell'apparato. Afferma il Garante che il MAC Address è sostanzialmente immodificabile e, date le caratteristiche (in particolare, la sua univocità su scala globale), consente di risalire, anche indirettamente, alla postazione corrispondente e di conseguenza all'utente che su di essa sta operando. Il Garante ha quindi ritenuto che il suo trattamento impone il rispetto della normativa sulla protezione dei dati personali e ne ha vietato l'utilizzo. Il provvedimento resta agganciato agli orientamenti espressi dal Garante della Privacy in applicazione delle disposizioni contenute negli artt. 11 e 13 del D.Lgs. n. 196/2003 che hanno influenzato per anni anche la giurisprudenza assestatasi - salvo alcune eccezioni - nel senso di non riconoscere in linea generale la legittimità dei controlli - pur "difensivi" - quando possano essere coinvolti, anche indirettamente, i dati sensibili del dipendente. In particolare, l'elemento che condiziona la inutilizzabilità di tali dati, a parere del Garante Privacy, quando ad essere coinvolta è ad esempio la casella di posta elettronica (il primo strumento di lavoro ad aver influenzato l'evoluzione nei provvedimenti del Garante in questa materia) è la legittima aspettativa di confidenzialità della stessa accompagnata, però, dall'assenza di una corretta informazione sulle modalità di uso e di un possibile, conseguente controllo (cfr. sul punto le Linee Guida del Garante già risalenti al 2007 e i Provvedimenti 139/2011; 308/2011). Mentre, per la giurisprudenza è la raccolta da parte del datore di lavoro dei dati di navigazione mediante accesso al terminale in uso al dipendente, anziché mediante accesso a file di backup (analogamente a quanto avviene con riguardo all'uso non corretto del telefono aziendale) che renderebbe illegittimo il comportamento datoriale, in assenza di policy e regolamenti interni (cfr. sul punto Cass., Sez. lav., 23 febbraio 2010, n. 4375, sent., in *Not. giur. lav.*, 2010, 176) (3).
Tuttavia qualcosa in questo ambito sta iniziando a cambiare grazie anche all'influenza che su questa materia ha esercitato il noto caso Barbalescu deciso all'inizio del 2016 dalla Corte Europea dei diritti dell'uomo (Sez. IV, 12 gennaio 2016, n. 61496/08). Nel caso specifico una Società aveva licenziato un dipendente per avere utilizzato la casella di posta aziendale per comunicazioni personali. Il lavoratore ha portato il caso alla Corte di Strasburgo la quale ha da un lato ritenuto a mag-

(2) In merito ai risvolti penalistici della disciplina e alla opportunità di ricercare sempre l'accordo con le rappresentanze sindacali ovvero di ricorrere all'autorizzazione amministrativa nel nuovo quadro normativo cfr. la recente prospettazione di un contrasto giurisprudenziale con il precedente costituito da Cass. Pen., Sez. III, 11 giugno 2012, n. 22611, in A. Scarcella, *Controllo dei lavoratori e sistemi di videosorveglianza: contrasto giurisprudenziale*, *Ipsoa Quotidiano Lavoro* 2 febbraio 2017.

(3) Per un recente richiamo agli orientamenti della Giurisprudenza e del Garante in materia di uso della posta elettronica aziendale cfr. E. Barraco, *Uso della posta elettronica aziendale a fini personali e accesso ai social network*, *D&PL, 46/2016*, 2751.

gioranza (sei voti contro uno), che vi era stata una violazione dell'articolo 8 della Convenzione europea dei diritti dell'uomo (diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza) ma ha altresì rilevato dall'altro che pur essendo stati coinvolti la vita privata del signor Barbalescu e la sua corrispondenza, il controllo svolto dal datore di lavoro nel caso specifico era da ritenere ragionevole nell'ambito e nel contesto del procedimento disciplinare avviato nei confronti del dipendente.
Nel secondo provvedimento si è, invece, richiesto al Garante di verificare la liceità di una App destinata a garantire - per esigenze di maggiore efficienza - la rilevazione delle presenze del personale impiegato "fuori sede" o presso clienti. L'uso dell'Applicazione - strutturata in modo da avere alcuni accorgimenti tecnici a garanzia della privacy del lavoratore - consente di avere un più efficace e rapido sistema di gestione delle timbrature, con possibile riduzione degli illeciti legati alle cosiddette "timbrature di comodo". Il Garante in questo caso ha ritenuto di precisare che, rispetto ai sistemi ordinari di rilevazione delle presenze - tramite i quali l'informazione sulla posizione geografica del lavoratore è del tutto indiretta statica ed invariabile - l'informazione geografica rilevata attraverso la nuova App è differenziata e specifica ed è posizionata all'interno di coordinate geografiche ogni volta diverse. In ragione di tale circostanza ed al fine di assicurare il corretto "bilanciamento degli interessi" che governa questo campo del diritto, il Garante ha ritenuto che anche tenendo conto delle finalità perseguite dalla Società - che restano solo quelle assimilabili ad una normale "timbratura" - il sistema è da considerare lecito - sempre previa notifica al Garante - solo se:
- è strutturato in modo da cancellare le coordinate geografiche della posizione del lavoratore conservando, eventualmente, il solo dato relativo alla sede di lavoro;
- è configurato in modo che sul dispositivo sia posizionata un'icona che indichi al dipendente che la funzionalità di localizzazione è attiva;
- è accompagnato da specifiche misure idonee a garantire che l'applicativo installato sul dispositivo del dipendente non possa effettuare trattamenti di dati ultronei (es. dati relativi al traffico telefonico, agli sms, alla posta elettronica o alla navigazione in internet o altro);
- sia fornita ai dipendenti un'informativa completa di tutti gli elementi previsti dall'articolo 13 del Codice Privacy. Informativa che non soddisfa, tuttavia, tutti i requisiti di "adeguata informazione" previsti dal nuovo art. 4 dello Statuto dei lavoratori qualora i dati eventualmente raccolti attraverso la App collegata allo "strumento di lavoro" vogliano essere utilizzati a fini disciplinari.

Quale limite per gli strumenti di lavoro

Come è possibile rilevare dal tenore dei provvedimenti sopra riportati, unitamente agli orientamenti dell'ultima giurisprudenza intervenuta in materia e qui brevemente commentata, nel contesto del nuovo art. 4 dello Statuto dei lavoratori il vero discrimine tra liceità e non liceità nell'uso a fini disciplinari dei dati raccolti attraverso gli strumenti di lavoro sarà di fatto costituito - nel contesto di nuove più rigorose policy interne - dalla valutazione della sua indispensabilità nel rendere la prestazione lavorativa e, vi è da ritenere, nella maggiore o minore idoneità del comportamento contestato a ledere il vincolo fiduciario alla base del rapporto di lavoro, anche in assenza di un danno significativo (su cui cfr. *ex plurimis* Cass. 18 settembre 2014, n. 19684).
Come affermato dai primi commentatori della novella, le implicazioni di natura organizzativa che derivano dal nuovo contesto normativo in cui il datore di lavoro sarà chiamato ad operare comporteranno, necessariamente, l'adozione di soluzioni che dovranno muoversi lungo "tre direttrici:
- trasparenza e informazione (consapevolezza del controllato);
- prevenzione (obbligo di adottare misure preventive volte a reprimere comportamenti illeciti e abusivi dei dipendenti, degradando il controllo di tipo successivo, cioè sull'illecito già consumato, ad *extrema ratio*);
- proporzionalità (che attiene alle modalità del controllo, che non deve mai essere svolto costantemente in modo indiscriminato e senza soluzione di continuità)" (4).
È questa la direzione che è stata intrapresa dalla prima giurisprudenza intervenuta in materia ad esempio di uso dei *social network*, espressasi sì in chiave evolutiva nella riaffermazione del fondamentale obbligo di fedeltà, ma ferma nel garantire che tale evoluzione deve essere direttamente colle-

(4) Cfr. A. Ingrao, *Il controllo a distanza realizzato mediante Social network*, LLI, 2, n. 1, 2016.

gata - come è facilmente intuibile - solo all'uso distorto degli strumenti di lavoro allorché dall'uso - necessitato - degli stessi possa derivare la compromissione dell'interesse del datore di lavoro alla diligente esecuzione della prestazione lavorativa (5).
Appare chiaro che, nel nuovo contesto normativo e come osservato anche dalla dottrina (6) il rispetto della procedura co-determinativa resta ancora oggi - peraltro - una fortissima garanzia per il datore di lavoro e deve poi essere accompagnato dalle policy e dai regolamenti interni, implementati *ad hoc* ovvero opportunamente aggiornati proprio in relazione alle modalità di uso degli strumenti di lavoro. Infatti tramite l'accordo sindacale o, in alternativa, grazie al provvedimento dell'autorità amministrativa è possibile regolare tra le parti tutta una serie di controlli particolarmente invasivi per la sfera privata dei lavoratori, ma anche le possibili conseguenze sanzionatorie.

Tale soluzione parrebbe quella più coerente con gli ultimi orientamenti della Cassazione in materia sopra riportati. Ma si prospetta anche la soluzione al momento preferibile nella organizzazioni complesse anche tenendo conto della direzione che pare stia intraprendendo anche l'autorità ispettiva (nonostante il diverso avviso della Cassazione espresso nella sentenza n. 19922/2016). Si pensi, infatti, solo per fare un esempio, alla recente Circ. n. 2/2016 del neo-costituito Ispettorato Nazionale del lavoro nella quale l'Ispettorato ha sancito che con riferimento all'installazione di apparecchiature di localizzazione satellitare GPS sulle autovetture aziendali - quindi su uno strumento di lavoro - è richiesto oggi obbligatoriamente il passaggio attraverso la procedura - sindacale o amministrativa - prevista dal comma 1 del novellato art. 4.

(5) Sul punto cfr. P. Salazar, *Facebook e rapporto di lavoro: a che punto siamo*, in questa *Rivista*, 2016, 2, 201.

(6) G. Zilio Grandi - M. Biasi, *Commentario breve alla riforma Jobs Act*, Milano, 2016, 727.