INSERT LAW TO CONTINUE 2019
CALL FOR PAPERS – Napoli 12-13 settembre 2019

Sessione: Sicurezza e protezione del dato digitale: problematiche e nuove prospettive giuridiche

*PAPER*
Sicurezza e protezione dell'informazione digitale nel rapporto di lavoro

SOMMARIO: 1.

L'inarrestabilità dei processi di innovazione tecnologica comporta effetti di dematerializzazione del lavoro e trasformazione in digitale attraverso forme di robotizzazione delle prestazioni via via crescenti e sempre più pervasive. Ne derivano due ordini di problemi.

Il *primo* incide sul piano della qualificazione dei nuovi modi di rendere la prestazione e delle connesse tutele onde comprendere se le attuali categorie giuridiche del lavoro subordinato/autonomo si prestano ad accogliere queste forme nuove di lavoro sia pure nelle tipologie variamente flessibili in cui spesso trovano declinazione, tema su cui la dottrina giuslavoristica discute già da tempo nella prospettiva di una rivisitazione degli attuali inquadramenti giuridici e che esula dai confini della predetta indagine

Il *secondo* problema -sul quale concentriamo l'attenzione- attiene alla persona del lavoratore e alla necessità di definire un sistema di protezione di tutte le informazioni che lo riguardano nel contesto della relazione di lavoro. Intendiamo fare riferimento al profilo della protezione dei dati personali che nella disciplina del diritto dei rapporti di lavoro ha mutato prospettiva all'indomani dell'ultima riforma del mercato del lavoro nota con il termine *Jobs Act* (legge delega n. 184/2014 e relativi decreti attuativi, nel caso che ci interessa si tratta del decreto legislativo n.151/2015). Ma anche per effetto del Regolamento Ue 2016/679 abrogativo del regolamento generale sulla protezione dei dati (dir.95/46/Ce) e del decreto legislativo n. 101/2018 (contenente norme di adeguamento della normativa nazionale alle disposizioni del Regolamento Ue 2016/679).

Schematizzando per punti le novità introdotte dai citati interventi normativi possiamo dire che: 1) la riforma del *Jobs Act* ha decisamente rafforzato il potere di controllo del datore di lavoro de-procedimentalizzandone l'esercizio. Esemplificativa, al riguardo, è la nuova disciplina dei controlli a distanza, storicamente ancorata, come noto, all'art. 4 dello Statuto dei lavoratori, ora modificato dall'art. 23 del d.lgs. n. 151/2015; 2) il Regolamento Ue 2016/679, entrato in vigore a maggio 2018, ha attribuito agli Stati membri il potere di intervenire *attraverso legge o tramite accordi collettivi* per assicurare la tutela dei diritti e delle libertà con riferimento al trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro, in ogni fase di esso e relativamente ad ogni aspetto che lo riguardi (assunzione, esecuzione del contratto di lavoro, pianificazione e organizzazione del lavoro, parità e diversità sul posto di lavoro, salute e sicurezza sul lavoro, cessazione del rapporto di lavoro, etc.); 3) il d.lgs. n. 101/2018 è stato emanato in adeguamento del Regolamento europeo del 2016, ma il legislatore non ha apportato modifiche di rilievo alla disciplina dei controlli e così, pur avendo la possibilità di intervenire nuovamente sulla norma nodale di cui all'art. 4 dello Statuto, ha preferito mantenere lo *status quo*.

Procedendo ad una analisi più dettagliata non si riscontrano novità rilevanti per quanto riguarda il trattamento di raccolta dei dati nella fase che precede l'assunzione e quindi la costituzione del rapporto. L'art. 113 del Codice *privacy* fa espresso rinvio all'art. 8 dello Statuto dei lavoratori e -ora- all'art. 10, d.lgs n. 276/2003, ambedue impositivi del divieto di raccogliere informazioni e svolgere indagini su fatti e circostanze non rilevanti ai fini della valutazione della professionalità del lavoratore ([1]).

1. Art. 10, d.lgs n. 276/2003: «E' fatto divieto alle agenzie per il lavoro e agli altri soggetti pubblici e privati autorizzati o accreditati di effettuare qualsivoglia indagine o comunque trattamento di dati ovvero di preselezione

Apparentemente nulla sembrerebbe cambiato anche dalla lettura dei successivi articoli del Codice privacy, 114, sul controllo a distanza, e 115, ampliato nella rubrica (ora intitolata *telelavoro, lavoro agile e lavoro domestico*), rimanendo costante il rinvio all'art. 4 dello Statuto dei lavoratori e addirittura pleonastica la disposizione dell'art. 115 quando impone al datore di lavoro un generico dovere di rispetto della personalità e della libertà morale del lavoratore.

In realtà, come si è anticipato, è mutato l'art. 4 St. lav., ora orientato ad un equilibrio assai più compensativo delle esigenze di tutela dell'impresa rispetto a quelle del lavoratore.

All'indomani dell'entrata in vigore del decreto legislativo n. 151/2015 attuativo della legge delega n. 183/2014 (cd. *Jobs Act*), l'art. 4 dello Statuto, difatti, da norma "chiave" della disciplina del potere di controllo datoriale é divenuto mera disposizione di "rinvio" alla disciplina generale sulla protezione dei dati personali.

Ciò premesso, lo studio in oggetto muove dall'analisi sistematica dell'art. 4 St. lav.., ([2]) per soffermarsi subito dopo sulle conseguenze derivanti dall'impatto delle novità legislative sulla persona del lavoratore nel contesto della evoluzione digitale e dei suoi effetti sulle relazioni di lavoro, in relazione al trattamento dei dati personali del lavoratore durante lo svolgimento dell'attività di lavoro, e più specificatamente alle modalità e ai limiti di utilizzo da parte del datore di lavoro dei dati medesimi.

Sotto il primo profilo, va preliminarmente inquadrata la disposizione di cui all'art. 4 dello Statuto dei lavoratori nella previgente formulazione. Il comma 1 si apriva sancendo il divieto "generale" del controllo a distanza dell'attività dei lavoratori. Il virgolettato vuole sottolineare la valenza del divieto, onnicomprensiva di qualunque forma di controllo a distanza. Tale periodo è stato abrogato e l'intero comma 1 riformulato alla stregua del vecchio secondo comma nella previsione che autorizza il controllo attraverso impianti audiovisivi e altri strumenti purché ricorrano le seguenti condizioni: esigenze produttive e organizzative, di tutela del patrimonio aziendale, di sicurezza sul lavoro, previa stipula di accordo con le organizzazione sindacali o autorizzazione amministrativa da parte dell'Ispettorato del lavoro.

La vera innovazione è tuttavia (anche) un'altra: l'integrale riformulazione del secondo comma e l'aggiunta di un nuovo terzo comma che liberalizzano completamente il potere di controllo datoriale. Il nuovo comma 2 dell'art. 4 St. lav. introduce espressamente una deroga all'applicazione del comma 1 là dove esonera il datore di lavoro dall'obbligo di motivare con una delle tre condizioni prima descritte (esigenze produttive e organizzative, di tutela del patrimonio aziendale, di sicurezza sul lavoro) e previa adozione della stipula di un accordo con le organizzazioni sindacali, in tutti i casi in cui la possibilità di effettuare controlli sull'attività dei lavoratori derivi dall'utilizzo degli *strumenti di lavoro*. In altri termini, non solo dall'uso di *pc,*

---

di lavoratori, anche con il loro consenso, in base alle convinzioni personali, alla affiliazione sindacale o politica, al credo religioso, al sesso, all'orientamento sessuale, allo stato matrimoniale o di famiglia o di gravidanza, alla eta', all'handicap, alla razza, all'origine etnica, al colore, alla ascendenza, all'origine nazionale, al gruppo linguistico, allo stato di salute nonche' ad eventuali controversie con i precedenti datori di lavoro, a meno che non si tratti di caratteristiche che incidono sulle modalita' di svolgimento della attivita' lavorativa o che costituiscono un requisito essenziale e determinante ai fini dello svolgimento dell'attivita' lavorativa. E' altresi' fatto divieto di trattare dati personali dei lavoratori che non siano strettamente attinenti alle loro attitudini professionali e al loro inserimento lavorativo».

([2]) Il comma 1 del predetto art. 4 dello Statuto subordina l'installazione di impianti audiovisivi e –non ben specificati- altri strumenti dai quali *può* derivare il controllo dell'attività dei lavoratori e quindi dei lavoratori medesimi al ricorrere di particolari esigenze aziendali (*1.* organizzative e produttive *2.* tutela della sicurezza del lavoro *3.* tutela del patrimonio aziendale) e al vaglio sindacale o amministrativo;

- il comma 2 prevede una espressa deroga alla disciplina procedimentale di cui al comma 1 per gli *strumenti utili al prestatore per rendere la prestazione lavorativa* nonché per gli *strumenti di registrazione degli accessi e delle presenze* sul luogo di lavoro;

- il comma 3 stabilisce che il datore possa utilizzare le informazioni raccolte ai sensi dei commi 1 e 2 *a tutti i fini connessi al rapporto di lavoro* a condizione di aver adeguatamente informato il lavoratore circa le modalità d'uso degli strumenti e di effettuazione dei controlli nel rispetto di quanto stabilito dal Codice sulla protezione dati personali.

*tablet, smartphone*, ma da qualsiasi altro apparecchio elettronico necessario allo svolgimento della prestazione, il datore di lavoro è libero di acquisire informazioni sulle modalità di esecuzione della prestazione, e sul lavoratore stesso. Inoltre può utilizzare le informazioni raccolte, come recita il comma 3 dell'art. 4, «per tutti i fini connessi al rapporto di lavoro» - ivi compresa, tanto per fare uno tra gli esempi che più frequentemente possono verificarsi, l'eventuale ipotesi del licenziamento del lavoratore scomodo- alla sola ed unica condizione –continua il co. 3 dell'art. 4- che dia adeguata informativa al lavoratore stesso in ordine alle modalità d'uso degli strumenti di lavoro ai sensi dell'art. 13 del Codice della *privacy* e nel generale rispetto di quanto da esso previsto. Come se il legislatore volesse dire: qui parliamo di mezzi di lavoro, non ci sono i margini per un controllo a distanza. E la logica è convincente: gli strumenti di lavoro sono elementi costitutivi della prestazione stessa, funzionali al suo stesso svolgimento, cioè l'esecuzione dell'obbligazione di lavoro è essa stessa il presupposto per l'utilizzo da parte del lavoratore degli strumenti di lavoro.

Neppure gli strumenti di registrazione delle presenze e degli accessi che hanno ormai sostituito i vecchi cartellini marcatempo necessitano delle condizioni prima elencate. I *badge* e i codici di accesso sono espressamente esonerati anch'essi dalle regole procedurali mentre prima la giurisprudenza forniva interpretazioni in un caso più restrittive (intorno agli anni '90 non si parla di controllo perché il controllo ha ad oggetto l'attività dei lavoratori e i codici di accesso sono deputati a registrare orari non movimenti dei lavoratori; intorno alla metà anni degli 2000 la giurisprudenza è più incline a configurare la fattispecie del controllo).

Ci si chiede allora: in via residuale si può delimitare la categoria degli altri strumenti di cui al comma 1, attraverso la categorizzazione di quelli utili a rendere la prestazione? La risposta non può che essere negativa in ragione dell'elevato grado di mutevolezza dovuto alla tipologia della prestazione e all'inarrestabilità del progresso tecnologico che non consente di circoscriverne la portata. Anche il vecchio concetto di "apparecchiature di controllo" creava non pochi problemi ermeneutici. La giurisprudenza vi faceva rientrare tutti gli strumenti che captavano le informazioni dei lavoratori e/o che erano in grado di acquisire informazioni riguardanti i lavoratori.

Dunque, in ordine al *secondo* profilo oggetto di questa analisi, concernente la sede applicativa, emerge in primo luogo il problema di individuare quali sono gli "strumenti utili a rendere la prestazione lavorativa" che possono essere sottratti al regime della procedimentalizzazione di cui al comma 1 dell'art. 4 -esteso agli "*altri strumenti dai quali può derivare il controllo dei lavoratori*- per rientrare nel cono applicativo della deroga di cui al successivo comma 2. Si pensi alla varietà di mezzi tecnologici di cui ci si avvale nello svolgimento dell'attività di lavoro, non solo la posta elettronica, gli apparecchi telefonici che si usano nei *call center*, che pure vengono continuamente aggiornati nei relativi *software*, ma per esempio ai sofisticati mezzi di geolocalizzazione come i braccialetti indossati dai dipendenti Amazon, i polsini dei lavoratori Motorola, che tracciano attraverso gli spostamenti dei lavoratori la qualità e quantità del lavoro svolto al fine di assegnare premi di produzione ([3]). Ancora, si pensi alle piattaforme *social network* in dotazione aziendale dei lavoratori-utenti per lo svolgimento di mansioni di *marketing* per il cui utilizzo al momento della stipula del contratto di lavoro vengono fornite al lavoratore le credenziali di accesso al profilo aziendale che restano in possesso dell'azienda e tramite le quali il datore può controllare l'attività dei lavoratori senza limiti spazio-temporali. Per non parlare, poi, della robotica, delle forme di intelligenza artificiale che sono espressione, tra l'altro, di processi di automazione incontrollabile tesi probabilmente a sostituire gran parte del lavoro umano.

([3]) Va citato il caso di Almaviva Contact S.p.A. che durante il quadriennio di crisi (2010-2014) ha sperimentato tecniche digitali di produzione: lean production (produzione snella) come metodo di produzione nei laboratori software allo scopo di minimizzare gli sprechi fino ad annullarli, per ottenere un aumento di produttività e un uso ottimale delle risorse umane. Le tecniche "lean" si basano su: sincronizzazione del flusso delle attività dettato interamente dalla domanda del cliente; standardizzazione delle azioni; tensione al continuo miglioramento, alimentata anche attraverso messaggi positivi (spirito di appartenenza, premi per performance); visualizzazione continua e gestione efficiente di informazioni (uso di bacheche e post-it per documentare statistiche, standard e avanzamenti produttivi); sviluppo di un processo strutturato di risoluzione dei problemi.

Su questo primo punto può dirsi sin d'ora che non pare rinvenibile alcuna differenza ontologica tra "gli altri strumenti" (comma 1) e "gli strumenti utili a rendere la prestazione" (comma 2). Sarebbe la **funzionalizzazione al lavoro propria degli strumenti prestazionali l'elemento di distinzione, in altri termini, il fatto che ogni mezzo di lavoro (*hardware*) è composto da più programmi informatici (*software*) idonei potenzialmente al controllo a distanza, fa sì che solamente i *software* non funzionali alla esecuzione della prestazione sarebbero passibili dei vincoli procedurali di cui al comma 1. Viceversa, quelli funzionalmente rivolti, *stricto sensu*, allo svolgimento dell'attività di lavoro rientrerebbero nel comma 2**. E' utile a questo riguardo il provv. del Garante 13 luglio 2016, n. 303 che definisce strumenti di lavoro quei «sistemi *software* che consentono, con modalità non percepibili dall'utente (cd. in *background*) e in modo del tuto indipendente rispetto alla normale attività dell'utilizzatore (cioè senza alcun impatto o interferenza sul lavoro del dipendente), operazioni di monitoraggio, filtraggio, controllo e tracciatura costanti e indiscriminati degli accessi a internet o al servizio di posta elettronica». Così disponendo l'Autorità ha chiarito che deve trattarsi di strumenti strettamente necessari a rendere la prestazione, mentre non è sufficiente che siano parzialmente utili allo scopo lavorativo. Anche il Ministero del lavoro ha affermato che se il mezzo di lavoro viene successivamente modificato tramite l'inserimento aggiuntivo di appositi *software* idonei a controllare il lavoratore occorre applicare le regole di cui al comma 2 dell'art. 4 (Comunicato stampa del Ministero del lavoro del 18 giugno 2015).

Il *secondo* problema si configura nel momento in cui, dopo aver accertato che si tratta di strumenti lavorativi, il comma 2 dell'art. 4 dello Statuto, derogando al regime di procedimentalizzazione imposto dal precedente comma 1 per gli impianti audiovisivi e gli altri strumenti dai quali è possibile che derivi una forma di controllo sui lavoratori, si limita semplicemente a rinviare alla disciplina generale sulla protezione dati contenuta nel Codice *privacy*. Sicché, a questo punto, ai fini della liceità del trattamento di controllo delle informazioni sui lavoratori raccolte tramite l'uso degli strumenti di lavoro, occorre verificare che il datore di lavoro si sia "*preventivamente"* conformato a quanto stabilisce il Codice *privacy* alla luce della neo-regolamentazione europea di cui al Regolamento Ue 2016/679. Cioè, in sintesi, abbia fornito regolare informativa *ex* art. 13 del Codice; predisposto l'organizzazione dell'impresa sin dalla fase della progettazione nel rispetto della disciplina sulla privacy (*privacy by design - privacy by default),* del criterio di *accountability,* e della valutazione di impatto della protezione dati *(privacy impact assessment-PIA);* abbia provveduto alla nomina della nuova figura del *Data protection officer-DPO (responsabile della protezione dati)*. Il mutamento di dialettica tra disciplina speciale e generale è evidente e pone in primo piano quella che ad oggi risulta la vera e propria innovazione culturale della riforma in materia di controlli sull'attività dei lavoratori: il ruolo chiave che assume ora la normativa sulla protezione dei dati nella gestione aziendale dei rapporti di lavoro sul presupposto che il controllo consiste in un trattamento di dati e il Codice *privacy* deve svolgere una funzione di prevenzione necessaria e imprescindibile.

Il che implica che il datore di lavoro trattando informazioni riguardanti i lavoratori ha l'obbligo di apprestare all'interno dell'impresa un modello di tutela della *privacy* "tarato" sulla prevenzione secondo gli enucleati principi della *privacy by design* e *by default*, della valutazione di impatto e della nomina di un responsabile della protezione dati personali (DPO) ma soprattutto della *accountability* del datore di lavoro. Non è opera facile adeguarsi alle nuove regole e non tanto per le imprese medie e grandi, quanto per le pmi che allo stato sono sfidate a sostenere costi troppo elevati per adeguare al GDPR (General Data Protection Regulation) i propri sistemi di conservazione e protezione dei dati personali. Occorrerebbero linee guida chiare nel percorso di adeguamento alle nuove regole e una semplificazione degli adempimenti che le PMI dovrebbero adottare.

Da questo punto di vista, infatti, il quadro degli adempimenti datoriali è piuttosto complesso. La protezione dei dati va osservata sin dalla fase della progettazione del processo aziendale (*privacy by design*) ovvero per l'intero ciclo di vita dei dati, dalla definizione delle modalità di trattamento sino al momento in cui avrà luogo la cancellazione attraverso la individuazione di misure di natura

tecnica e anche organizzativa idonee a ridurre al minimo il trattamento di dati (cd. principio di minimizzazione). La previsione evoca i criteri della «prevenzione dei rischi alla fonte» e della programmazione della prevenzione finalizzata alla «eliminazione e/o riduzione dei rischi al minimo in relazione alle conoscenze acquisite in base al progresso tecnico», i quali rappresentano alcune fra le misure generali di tutela che il datore di lavoro è tenuto ad adottare ai sensi dell'art. 15, co. 1, lett. *b), c), e)*, del d.lgs. n. 81/2008. Lo stesso può dirsi per il criterio della valutazione d'impatto (*privacy impact assessment-PIA*), che, nel prevedere l'obbligo, per il responsabile del trattamento, di effettuare una valutazione circa l'impatto che i trattamenti possono determinare sugli interessati – prima che gli stessi abbiano inizio nei casi in cui l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le sue finalità, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche – richiama il principale (e non delegabile) obbligo del datore di compiere la valutazione di tutti i rischi e di redigere il relativo documento contenente la programmazione, l'individuazione dei rischi e delle misure da predisporre, secondo quanto stabilito dagli artt. 17 e 28, d.lgs. n. 81/2008.

L'art. 33 (ora art. 35 del Regolamento 2016/679) stabilisce, difatti, che la valutazione d'impatto è svolta dal responsabile del trattamento previa consultazione con il responsabile della protezione dei dati (se designato) (par. 2) e si conclude nella redazione di un documento che contiene la descrizione delle operazioni di trattamento previste e delle finalità del trattamento, una valutazione della necessità e proporzionalità dei trattamenti con riguardo alle finalità, una valutazione dei rischi per i diritti e le libertà degli interessati, nonché le misure previste per affrontare i rischi, comprese le garanzie, le misure di sicurezza da predisporre (par. 3).

Quanto, infine, alla istituzione del responsabile della protezione dei dati personali (art. 37-*Data protection Officer-DPO*) si tratta di una figura del tutto nuova nel panorama italiano della *privacy*, da non confondere con il responsabile del trattamento che è preposto dal titolare allo svolgimento di tutte le operazioni sui dati, tant'é che nel Regolamento Ue il DPO è invece un soggetto interno o esterno all'azienda, in possesso di competenze specialistiche in materia, che viene designato dal responsabile e dall'incaricato del trattamento per lo svolgimento di tutte le questioni attinenti alla protezione dei dati. Nell'ambito dei compiti e delle funzioni che deve svolgere, è tenuto a monitorare, in via generale, l'osservanza del Regolamento, a curare anche l'aspetto della formazione del personale, può fornire consulenza in merito alla valutazione d'impatto – nel caso gli venga richiesto – e deve valutare i rischi inerenti al trattamento, tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento (ora artt. 37, 38, 39 del Regolamento 2016/679).

L'ultima -e fondamentale- questione attiene alla utilizzabilità delle informazioni raccolte che –recita il comma 3 dell'art. 4- può avvenire per "*tutti i fini connessi al rapporto di lavoro*". Come a dire: l'utilizzo delle informazioni personali sui lavoratori trova il proprio limite nella liceità del trattamento del controllo. Accertato il limite della stretta funzionalità alla prestazione, e del rispetto della disciplina generale sulla protezione dati, sembra di poter convenire che il datore non abbia altri limiti nell'utilizzo dei dati raccolti. Pertanto, *quid juris* nel caso di illecita raccolta? Il datore potrà utilizzare i dati raccolti illecitamente? L'art. 171 del Codice privacy prevede che nei casi in cui il datore di lavoro violi le disposizioni di cui agli articoli 4, comma 1, e 8 della legge 20 maggio 1970, n. 300, si applicano le sanzioni pecuniarie di all'art. 38 St. lav. Ma per il comma 3 non si prevede né un'estensione dell'art. 38 né una sanzione *ad hoc*. Il motivo probabilmente sta nel fatto che il nuovo Codice dispone la regola della "*inutilizzabilità"* dei dati trattati in violazione dei principi di liceità e correttezza, pertinenza e non eccedenza, conservazione (art. 2-decies, d.lgs. n. 101/2018). Ne consegue, pertanto, che, in caso di utilizzo improprio dei dati il lavoratore potrà adire in primo luogo il Garante, per esempio nelle more dell'impugnazione di un atto di licenziamento per motivo disciplinare illegittimo o giusta causa quando a fondamento della causa di licenziamento il datore abbia addotto un fatto "costruito" mediante informazioni raccolte illecitamente o comunque in modo lecito ma che utilizza per finalità illecite quali appunto il licenziamento. La pronuncia dell'Autorità costituirà mezzo di prova che il lavoratore potrà esibire nel giudizio civile

orinario, sarà il mezzo con il quale il lavoratore dimostrerà l'insussistenza materiale del fatto contestato, ai fini della reintegra (art. 3, comma 2, d.lgs. n. 23/2015). Ma in ogni caso, venga o meno adita l'Autorità Garante per accertare la liceità o illiceità del controllo datoriale sui lavoratori tramite l'uso degli strumenti di lavoro, qualora il datore utilizzi le informazioni raccolte non adempiendo agli obblighi procedurali richiesti dalla regolamentazione generale sulla protezione dei dati personali, per qualunque scopo connesso al rapporti di lavoro, come per esempio il licenziamento del dipendente controllato, l'indagine del giudice ordinario dovrà allargarsi a verificare il criterio della utilizzabilità/inutilizzabilità dei dati, alla stregua del quale soltanto potrà pronunciarsi per l'eventuale legittimità/illegittimità dell'atto posto in essere dal datore di lavoro.

Infatti, se il motivo o la giusta causa si fonda su  dati non utilizzabili ai sensi dell'art. 2.-decies d.lgs. n. 101/2018, ciò andrà ad incidere sulla sussistenza materiale del fatto contestato che ai sensi dell'art. 3, comma 2, d.lgs. n. 23/2015 (tutele crescenti) deve essere provata in giudizio ai fini del giudizio di reintegra sempre che si rientri nei requisiti dimensionali di cui all'art. 18, commi 8 e 9, giacchè - si ricorda – quella del licenziamento disciplinare per g. causa o g.m.s. è l'unica ipotesi, fra quelle per le quali è ammessa la reintegra, che l'art. 9, comma 1, d.lgs. n. 23/2015, assoggettata ai limiti dimensionali stabiliti dall'art. 18 dello Statuto.

Seguono *slides* di rappresentazione del dato normativo