

Controllo a distanza e diritto alla protezione dei dati. Sulla complementarità dei due sistemi normativi

Alessandra Ingrao

1. Un ricordo di Riccardo Del Punta

Fin dalla prima conoscenza con Riccardo Del Punta – a Modena, al convegno in memoria di Marco Biagi – pochi anni prima della riforma dell’art. 4 St. lav. mi parse attanagliato dalla ricerca di un elemento di equilibrio da inserire nella ricetta che stava studiando, che poi sarebbe confluita, assunte le vesti di testo normativo, nella integrale sostituzione dell’art. 4 St. lav.

Tra una relazione e l’altra, Riccardo Del Punta osservava, con tono polemico, benché ammorbidito dal suo accento pisano, che le norme statutarie del Titolo I, che limitano potere d’indagine e controllo, potevano solo «fare tenerezza» al cospetto della sofisticazione delle nuove tecnologie che consentono, di fatto, un tracciamento totale della prestazione e una scomposizione della persona capillare.

Fu quella battuta – che riusciva, simpaticamente, a condensare in poche lettere la complessità della questione di fondo – a instillare in me il dubbio che le soluzioni di equilibrio – la ricetta della «proporzionalità» del potere di controllo che R. Del Punta andava cercando – potevano essere trovate anche fuori dallo Statuto dei lavoratori, aggiungendo alla prospettiva del divieto imperativo, una regolazione di principio, maggiormente flessibile e più adatta ad adeguarsi in concreto al nuovo che avanza.

Qualche tempo dopo, varato l’art. 4 St. lav. e pubblicati diversi lavori di R. Del Punta di spiegazione della riforma, capii che nella ricetta che era stata trovata

Alessandra Ingrao, University of Milan, Italy, alessandra.ingrao@unimi.it, 0000-0001-7991-4785

Referee List (DOI 10.36253/fup_referee_list)

FUP Best Practice in Scholarly Publishing (DOI 10.36253/fup_best_practice)

Alessandra Ingrao, *Controllo a distanza e diritto alla protezione dei dati. Sulla complementarità dei due sistemi normativi*, © Author(s), CC BY 4.0, DOI 10.36253/979-12-215-0507-8.38, in William Chiaromonte, Maria Luisa Vallauri (edited by), *Trasformazioni, valori e regole del lavoro. Scritti per Riccardo Del Punta*, pp. 637-653, 2024, published by Firenze University Press, ISBN 979-12-215-0507-8, DOI 10.36253/979-12-215-0507-8

l'elemento di ri-equilibrio del potere di controllo a distanza – legittimato a raccogliere dati «a tutti i fini connessi al rapporto di lavoro» – risiedeva nel rinvio al d.lgs. 196/2003. La protezione dei dati del lavoratore che poggia sulla trasparenza della raccolta, sulla sua minimizzazione, finalità e proporzionalità, segnava un orizzonte che andava esplorato con più convinzione rispetto al passato.

Nelle pagine che seguono si indagano le ripercussioni di questi principi sul potere di controllo a distanza, identificando i (nuovi) limiti del potere, come disciplinato dall'art. 4 St. lav. a seguito della sua modifica ad opera del d.lgs. 151/2015 (art. 23), attuativo del cd. *Jobs Act*.

L'occasione è altresì idonea a stilare un primo bilancio della riforma della disposizione statutaria per verificare se anche la giurisprudenza abbia colto la rilevanza sistematica del diritto alla protezione dei dati personali del lavoratore che incide notevolmente sull'esercizio del potere di controllo, condizionandolo ulteriormente al fine di soddisfare il bilanciamento costituzionale di cui all'art. 41, co. 2, Cost.

2. La «doppia faccia» dell'art. 4 St. lav.: limiti al potere e vincoli all'utilizzabilità dei dati e delle prove

La scelta di regolare l'orizzonte della consultabilità/utilizzabilità dei dati raccolti e memorizzati negli strumenti tecnologici dal datore di lavoro costituisce sicuramente la punta più avanzata della riforma che, da un lato fa cadere quella che R. Del Punta definiva «l'ipocrisia» della vecchia norma, ma che dall'altro lato, impone di comprendere se la nuova disposizione legittimi il datore di lavoro a sorvegliare l'attività lavorativa per il tramite delle tecnologie¹.

La riforma dell'art. 4 St. lav. permette di cogliere più facilmente la doppia anima dell'art. 4 St. lav., che sin dal 1970, poteva essere raffigurato come un Giano bifronte, un'entità divina dal doppio volto.

Con la prima faccia, la disposizione era ed è volta a circoscrivere l'esercizio del potere di sorveglianza tecnologica, imponendo limiti sostanziali e procedurali – continuando a istituzionalizzare un contropotere collettivo, rivolto a codeterminare l'installazione di alcuni (anche se non per tutti gli) strumenti di videoripresa e controllo – volti a comprimerne l'autonomia organizzativa del datore di lavoro in ragione della tutela dei diritti della persona.

Con la seconda faccia, l'art. 4 St. lav. è norma che condiziona e limita l'utilizzabilità delle informazioni raccolte al fine di modificare o estinguere il rapporto di lavoro.

In assenza della disposizione statutaria, infatti, gli esiti delle rilevazioni effettuate dal datore di lavoro, consentirebbero di acquisire qualsiasi informazione sull'attività della persona che lavora, delle sue attitudini e dei suoi comportamenti solutori (salvo il divieto contenuto nell'art. 8 St. lav.).

¹ Del Punta 2016; Tullini 2017; Nuzzo 2018; Dessì 2018; per altri riferimenti si consenta di rinviare a Ingraio 2018. Sartori 2020; Pisani, Proia, Topo 2022.

L'art. 4 St. lav. infatti, lungi dal legittimare un regime di libera utilizzabilità dei dati, ne scolpisce piuttosto uno a «utilizzabilità vincolata», dove i «pesi» e i «vincoli» sulle informazioni devono essere determinati dallo stesso datore di lavoro in conformità all'art. 4 St. lav. e al Regolamento UE/2016/679 (che pur essendo direttamente applicabile è stato recepito nel d.lgs. 196/2003 ad opera del d.lgs. 101/2018). Nello specifico, il rinvio esplicito contenuto nell'art. 4, co. 3, St. lav. al sistema *privacy* rende l'espletamento dei doveri datoriali di protezione dei dati personali dei lavoratori (su cui diffusamente *infra* par. 3) condizioni di utilizzabilità dei dati². Diviene dunque rilevante comprendere il contenuto delle condizioni di utilizzabilità poste dall'art. 4 St. lav.

3. Una lettura integrata: Il controllo a distanza come trattamento di dati personali del lavoratore.

L'esercizio del potere di controllo a distanza, a prescindere dalla successiva utilizzazione dei dati da parte del datore di lavoro, deve risultare rispettoso del diritto alla *privacy* del lavoratore³.

Il moderno concetto di *privacy* – definito e disciplinato dal d.lgs. 30 giugno 2003, n. 196 come modificato dal Regolamento 2016/679/EU che sostituisce la Direttiva 1995/45/CE⁴ – non coincide con l'originaria impostazione privatistica un po' intransigente di «pretesa ad essere lasciati soli» (Carnelutti 1955; De Cupis 1959), né tanto meno con il diritto a mantenere riservata la propria sfera intima da sguardi indiscreti di terzi. Piuttosto occorre pensare al diritto alla protezione dei dati personali delle persone fisiche come un diritto «gentile» che è sempre capace di «cedere il passo» ad altri interessi legittimi la cui sod-

² La natura di norma processuale dell'art. 4 St. lav. comporta un condizionamento dei poteri istruttori del giudice civile che è obbligato a dichiarare inammissibile il materiale probatorio (digitale) raccolto in violazione dei limiti in esso contenuto come integrato dalla disciplina *privacy*. Nel giudizio penale – ancora oggi instaurabile per la continuità dell'illecito previsto dall'art. 61, co. 2, d.lgs. 101/2008 e art. 38 St. lav. – la norma opera parallelamente alla previsione dell'art. 191 c.p.p. Gamba 2016; Barbieri 2017, 183-208.

³ L'acquisizione è condivisa da una larga parte della giurisprudenza di merito *post Jobs Act*. Si segnalano in particolare Trib. Vicenza 28 ottobre 2019; Trib. Roma 13 giugno 2018; Trib. Padova 22 gennaio 2018 che riconoscono espressamente che il controllo a distanza, rappresenta una fase del trattamento dei dati personali, e come tale deve rispettare i principi dettati dalla normativa, ossia i principi di liceità, di correttezza, di necessità, di determinatezza della finalità perseguita, di pertinenza, di completezza, di non eccedenza. Prima del *Jobs Act* a quanto consta soltanto Trib. ferrara 27 agosto 2012 aveva dichiarato illegittimo il controllo effettuato sul computer aziendale in uso al dipendente per violazione sia dell'art. 4 St. lav., poiché la sorveglianza effettuata all'infuori dei canoni di lealtà e correttezza e non per scopi determinati, espliciti e legittimi *ex art. 11, d.lgs. n. 196 del 2003*, costituisce un trattamento illecito di dati personali. Si dirà meglio *infra* che, al di là di queste pronunce di merito, la giurisprudenza di legittimità continua ad accreditare la tesi del controllo difensivo esercitato dal datore di lavoro in violazione sia della norma statutaria che della normativa *privacy*. In dottrina, *contra*, con argomenti differenti Marazza 2016; Maresca 2017, 21; Proia 2016.

⁴ Per tutti si veda Bellavista 2007.

disfazione presuppone, nella società dell'informazione, la circolazione dei dati. Dovendo l'individuo, nei vari contesti in cui si esplica l'attività umana, aprire la propria sfera identitaria all'interrelazione coi terzi, la normativa in parola intende assicurare che la persona interessata dal trattamento dei suoi dati, che le appartengono in una relazione quasi dominicale, sia consapevole degli scopi del loro utilizzo e ne resti padrona, potendovi accedere ed opporsi al trattamento realizzato da terzi per finalità trasparenti e predeterminate (Rodotà 1997, 698).

Sebbene, il rinvio al codice della *privacy* sia contenuto esclusivamente nel co. 3 dell'art. 4 St. lav., è da intendere in senso ampio la complementarità tra i due sistemi normativi, essendo possibile «innestare» interpretativamente il rinvio su ogni disposizione del Titolo I che limiti indagini, controlli e perquisizioni sui lavoratori, dal momento che tali comportamenti datoriali sono diretti a trattarne i dati (i cd. «innesti regolativi»; Chieco 2000, spec. 20).

La convergenza regolativa incide sulle condizioni di legittimità dell'esercizio del potere-trattamento e condiziona l'utilizzabilità degli esiti delle rilevazioni datoriali. Del resto, non è nuova l'acquisizione in base alla quale il sistema di protezione della *privacy* degli individui aggiunga garanzie ulteriori rispetto allo Statuto dei lavoratori, procedimentalizzando le modalità di realizzazione del trattamento delle informazioni da parte del datore di lavoro, sin dal momento della scelta e installazione della tecnologia di controllo-trattamento. Il legislatore del 2015, allora, si sarebbe limitato a richiamare l'attenzione degli interpreti su tale cruciale aspetto (Tullin 2017, 97 sgg.).

Quel che merita un'attenzione rafforzata è l'approccio che l'Unione Europea ha adottato per garantire l'obiettivo della protezione dei dati degli individui che, nell'attuale di fase di digitalizzazione, non solo dei contesti lavorativi, è divenuto tema centrale e d'impatto geo-politico. Sebbene sia qui possibile enucleare la nuova strategia solo per punti, occorre prendere le mosse dal progressivo abbandono della precedente impostazione autorizzatoria della Direttiva 1995/45/CE, in favore di una incentrata sul concetto di *accountability* o responsabilizzazione del titolare del trattamento (art. 5 Reg.), ossia di chi determina finalità e mezzi dello stesso.

La logica del Regolamento può essere facilmente compresa dai giuslavoristi perché essa ricalca quella tutta europea della prevenzione del rischio delle lavorazioni e dell'organizzazione in materia di protezione della salute e della sicurezza nei luoghi di lavoro. In altri termini, nel Regolamento 2016/679/UE si assume che la digitalizzazione delle organizzazioni produttive può esporre a rischio i diritti fondamentali del lavoratore di libertà e dignità. Le cui informazioni personali vengono catturate, immagazzinate per poi essere potenzialmente utilizzabili per scopi incogniti e indeterminati per produrre effetti giuridici sul rapporto di lavoro. Partendo da tale assunto il Regolamento obbliga il titolare del trattamento a minimizzare, o se possibile eliminare, tale rischio, auto-limitando le modalità di realizzazione del trattamento (controllo a distanza), come meglio si dirà in seguito. Il datore di lavoro *accountable*, dunque, dovrà adottare ed essere in grado di dimostrare, un modello organizzativo che contempra misure giuridiche, organizzative e tecniche adeguate a fronteggiare il rischio di lesione dei diritti che può derivare dall'esercizio del potere di controllo a distanza.

È dovere del datore di lavoro, quando siano effettuati controlli a distanza ⁽⁵⁾ predisporre la valutazione d'impatto privacy (art. 35 Reg.) un documento di mappatura dell'apparato tecnologico strumentale che descriva gli scopi e i mezzi dei trattamenti di dati personali, i rischi per i diritti nonché le misure di protezione intraprese. Benché ad oggi nelle sentenze non vi sia traccia della richiesta di esibizione di tale documento per vagliare la legittimità del controllo realizzato, non si dubita che ricada sul datore di lavoro l'onere di provare la suddetta mappatura nonché di aver strutturato i dispositivi di controllo *ab origine* ⁽⁶⁾ in ottemperanza ai principi del trattamento di legittimità, finalità, minimizzazione e trasparenza. Ciò a prescindere dalla distinzione tra strumenti di controllo e di lavoro contenuta nei primi due commi dell'art. 4 St. lav. (su cui si tornerà *infra* par. 5).

3.1. Legittimità del trattamento dei dati tra base giuridica e principi

Alla luce della logica precauzionale del Regolamento, la legittimità del controllo a distanza è da vagliare attraverso un giudizio bifasico: esso deve essere legittimato a monte dalla ricorrenza di una condizione di legittimità del trattamento dei dati normativamente prevista, la cd. base giuridica (art. 6 Reg.) e, in secondo luogo, le sue modalità di esercizio devono risultare conformi ai principi (art. 5 Reg.).

Il controllo a distanza, già nel regime previgente, necessitava di una base giuridica diversa dal consenso del lavoratore, che non avrebbe potuto essere prestato genuinamente in un rapporto giuridico impari⁷. Il suo fondamento di liceità infatti consiste piuttosto nel «perseguimento del legittimo interesse» del datore di lavoro che non è considerabile come un effetto automatico della condizione di dipendenza lavorativa del prestatore, ma piuttosto come il frutto di una scelta ragionata dal datore di lavoro da cui si desuma la ricorrenza in concreto delle esigenze tassativizzate dall'art. 4 St. lav., esigenze organizzative, produttive, di salute e sicurezza del lavoro e di tutela del patrimonio aziendale le quali, se non esplicitate nell'accordo sindacale o nell'autorizzazione amministrativa (art. 4, co. 1), dovranno potersi desumere dall'informativa privacy (ex art. 4, co. 3) consegnata al lavoratore nel caso degli strumenti di cui al co. 2, oppure dalla valutazione d'impatto *privacy*.

⁵ La Valutazione d'impatto è obbligatoria in caso di controllo a distanza e di profilazioni digitali finalizzate alle decisioni automatizzate algoritmiche (provvedimento prescrittivo Garante privacy 2018).

⁶ Il Regolamento 2016/679/UE dà per assodato il carattere conformativo della tecnologia che essendo artefatto umano può essere programmata *by design* e *by default* in modo da incorporare per impostazione predefinita il rispetto dei diritti della persona.

⁷ Gruppo di lavoro ex art. 29, parere n. 2/2017 *on data processing at work*, adottato l'8 giugno 2017, WP249, 7 e 14. Cfr. altresì Id., opinione n. 6/2014 che evidenzia la necessità che il titolare del trattamento esegua un vero e proprio «test» sulla base di diversi fattori: la natura del legittimo interesse, la natura dei dati trattati, il tipo di pregiudizio che può derivare all'interessato (l'azione disciplinare) e la sua ragionevole aspettativa. Cfr. Sitzia 2016.

Dalla base giuridica si differenziano i principi, la cui concretizzazione imprime vincoli sulle modalità di realizzazione del controllo e sui suoi scopi concreti, ossia sulle finalità per le quali è esercitato.

Il fatto che il co. 3 dell'art. 4 St. lav. stabilisca che l'utilizzabilità dei dati è possibile «a tutti i fini connessi al rapporto di lavoro» non significa che la norma legittimi l'esercizio di un potere di controllo a distanza multifunzionale e non sorretto da una predeterminazione di scopo, permettendo al datore di lavoro di «rastrellare» enormi quantità d'informazioni sulla persona e sulla prestazione lavorativa riservandosi il diritto di scegliere *ex post* lo scopo di utilizzo dei dati (disciplinare, formativo, retributivo, gestionale ecc.).

Una simile lettura non solo sarebbe contraria rispetto alle riflessioni della dottrina civilistica per cui poteri privati completamente liberi nei fini devono considerarsi illeciti a causa della loro intrinseca arbitrarietà (Lener 1985), ma contraddirebbe altresì il principio di limitazione delle finalità, pietra angolare di tutta la costruzione del sistema a protezione dei dati, in base al quale lo scopo di ciascun controllo a distanza deve essere determinato preventivamente, esplicitato nell'informativa, rispettato per tutto il trattamento fino alla cancellazione dei dati. Cosicché deve essere noto al lavoratore sin dall'installazione o consegna dello strumento quale sia l'effetto (modificativo o estintivo) che il controllo può importare sul rapporto di lavoro. La predeterminazione delle finalità comporta poi un vincolo di utilizzabilità dei dati.

Il trattamento deve poi essere improntato alla minimizzazione, in quanto vanno raccolti solo dati personali necessari per raggiungere gli scopi prefissati e noti al lavoratore. La minimizzazione del trattamento, imprime al potere di controllo a distanza un canone di proporzionalità da valutare in concreto rispetto ai suoi scopi. Da tale principio si ricava un divieto di controllo continuativo sulla prestazione che tenda al tracciamento e alla profilazione digitale, finalizzata a desumere il rendimento del lavoratore (cfr. art. 22 Reg.).

Infine, il controllo a distanza non può essere occulto, come anche diverse sentenze di merito hanno sostenuto⁸ seguite da parte di giurisprudenza di

⁸ L'informazione dell'esistenza di un controllo è necessaria sia in caso di controlli effettuati ai sensi del comma 1 sia in caso di controlli di cui al comma 2 della disposizione (sul punto espressamente Trib. Vicenza 28 ottobre 2019; Trib. Milano 13 maggio 2019; Trib. Torino 19 settembre 2018; Trib. Roma 13 giugno 2018; Trib. Padova 19 gennaio 2018; Trib. Pescara 25 ottobre 2017). L'informazione deve poi essere esaustiva ed adeguata, cioè in grado di portare il lavoratore a conoscenza della possibilità di essere assoggettato ai controlli da parte del datore di lavoro, oltre che delle modalità e dei limiti degli stessi, non potendo ridursi tale obbligo ad un mero adempimento formale (Trib. Vicenza 28 ottobre 2019, cit.; Trib. Torino 19 settembre 2018, cit.). Inoltre, si consideri che non è informativa «adeguata» ex art. 4, co. 3, né il documento che prescrive direttive riguardanti tutte le tipologie di strumenti impiegati nell'organizzazione aziendale, nell'ambito di un modello di organizzazione e gestione previsto dal d.lgs. n. 231/2001 (Trib. Torino 19 settembre 2018) né tanto meno il regolamento aziendale che si limiti a specificare che personal computer e casella di posta elettronica assegnati al lavoratore sono strumenti di lavoro, senza tuttavia indicare l'eventualità che attraverso questi strumenti l'azienda può controllare l'attività lavorativa Trib. Vicenza 28 ottobre 2019, cit.

Cassazione⁹, giacché l'intero procedimento di trattamento deve rispondere al principio di trasparenza, rafforzato dalla previsione di cui all'art. 4 co. 3 il quale stabilisce che sia data al lavoratore una informativa preventiva che lo renda consapevole della possibilità di subire il monitoraggio nonché degli usi consentiti degli strumenti¹⁰.

Corollario del principio di trasparenza è il diritto d'accesso ai dati raccolti che costituisce il tramite per l'esercizio degli altri diritti, tra cui anche quello di opposizione al trattamento.

Si comprende in ultima analisi la rilevanza organizzativa del diritto alla protezione dei dati dei lavoratori nell'ipotesi in cui la tecnologia sia impostata per raccogliere i dati al fine di controllare anche preterintenzionalmente la prestazione lavorativa.

4. Conseguenze applicative della lettura integrata: il controllo a distanza per finalità disciplinari

Dalla configurazione del potere datoriale di controllo a distanza come trattamento di dati personali dei lavoratori discendono implicazioni utili a risolvere una serie di problemi lasciati aperti dal testo riformato dell'art. 4 St. lav. su cui dottrina e giurisprudenza si sono misurata in questi quasi otto anni di applicazione della disposizione senza tuttavia approdare a soluzioni condivise.

Di seguito la trattazione approfondisce la finalità disciplinare di controllo a distanza in quanto essa è la più diffusa. Ciò non significa che il controllo non sia realizzabile per scopi differenti, come quello retributivo, formativo o di protezione della salute e della sicurezza.

L'art. 4, co. 3, St. lav. che il monitoraggio tecnologico della prestazione lavorativa sia il presupposto dell'esercizio del potere disciplinare (artt. 2106 c.c. e 7 St. lav.), seppur entro limiti determinati.

Il primo deriva dalla delimitazione della base giuridica che giustifica e sorregge l'interesse legittimo del datore di lavoro ad effettuare il controllo. Nel te-

⁹ Per Cass. 19 settembre 2016, n. 18302 l'indicazione inserita nel regolamento aziendale di effettuare periodicamente i salvataggi dei dati su supporti magnetici e/o di rete e la conservazione degli stessi in luogo idoneo non può considerarsi una informazione adeguata, in quanto non comporta che i lavoratori 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. Inoltre, la Corte di Cassazione, nella prima pronuncia applicativa dell'art. 4, l. n. 300/1970 novellato, ha ritenuto valida l'informativa fornita ai dipendenti circa le modalità di uso degli strumenti di lavoro e di effettuazione dei controlli anche se data ai dipendenti anteriori al d.lgs. n. 151/2015 (Cass., sez. lav., 24 febbraio 2020, n. 4871).

¹⁰ Sulla comprensibilità dell'informativa e sul collegato tema della quantità d'informazioni che occorre dare al lavoratore cfr. Tullini 2017, 117; Maresca 2017, 24 per il quale il datore di lavoro non deve redigere «un manualetto d'istruzioni». Il Garante per la protezione dei dati personali, provvedimento del 19 marzo 2015, *Linee guida in materia di trattamento di dati personali per profilazione on line*, [doc. web n. 3881513], ha caldeggiato la scomposizione della informativa in due testi: uno approfondito ed esteso e l'altro sintetico.

sto dell'art. 4 St. lav. si possono identificare almeno due macro esigenze tassative atte a legittimare il trattamento dei dati sull'adempimento della prestazione lavorativa e degli obblighi di disciplina (art. 2104, co. 2, c.c.). Infatti accanto alla «tutela del patrimonio aziendale» sono nominate altresì le macro esigenze «organizzative e produttive».

Entrambe sottendono la tutela di una posizione soggettiva patrimoniale del datore di lavoro, tuttavia occorre procedere a trattazione separata delle due basi giuridiche poiché il controllo al fine di preservare il patrimonio aziendali da comportamenti illeciti e dannosi dei lavoratori, eventuali e occasionali, assume una configurazione differente rispetto al monitoraggio della produttività e del rendimento individuale che presuppone un monitoraggio costante.

La novella del 2015 ha stabilito che il patrimonio aziendale possa essere tutelato anche attraverso controlli a distanza sui comportamenti dei lavoratori disciplinarmente rilevanti dei lavoratori¹¹.

L'acquisizione non è di per sé una novità se si considera che da oltre vent'anni la giurisprudenza ribadisce il suo orientamento sul «controllo difensivo», in base al quale l'art. 4 St. lav. limita il controllo sull'attività lecita del prestatore, ma non su quella illecita che perciò se «catturata» da strumenti digitali installati in violazione delle norma statutaria può costituire prova ammissibile di un fatto disciplinarmente rilevante¹². L'orientamento in parola, però, risente di una visuale parziale dei giudici, protesi a far salva la prova della giusta causa di licenziamento *ex post*, senza però preoccuparsi che questa sia il frutto di una sorveglianza esercitata *ex ante* su diversi lavoratori che non hanno commesso alcun illecito¹³.

Sta proprio qui la differenza tra la versione giurisprudenziale del controllo difensivo della tutela del patrimonio aziendale e la lettura integrata del controllo a distanza improntata ai principi di trasparenza, finalità e proporzionalità del monitoraggio.

¹¹ Sia attraverso impianti di video sorveglianza sia attraverso altri strumenti di controllo, di lavoro o di registrazione di accessi e delle presenze che incorporino funzionalità di controllo. Sulla distinzione si tornerà *infra* par. 5, basti qui dire che nella prima ipotesi la ricorrenza della base giuridica tutela del patrimonio aziendale sarà verificata in concreto attraverso la procedura codeterminativa sindacale o in sua assenza dall'organo amministrativo, mentre, nella seconda ipotesi, il datore di lavoro è responsabile di dimostrare la ricorrenza in concreto del suo «legittimo interesse» e descrivendolo nella «valutazione d'impatto privacy» (art. 35 Reg.). Non si tratta tuttavia di una *probatio diabolica*, giacché gli studi sociologici individuano il *cyberslacking* o *cyberloafing* ossia l'uso per fini non lavorativi delle risorse digitali, come un notevole rischio che l'impresa è tenuta a sostenere, soprattutto nell'eventualità che i dispositivi di lavoro siano «utilizzati» direttamente dal lavoratore, cfr. Friedman 2000.

¹² In termini parzialmente analoghi Tullini 2017, 103, che osserva «non è chiaro se» l'installazione per esigenze di tutela del patrimonio aziendale «includa oltre gli illeciti di natura extra-contrattuale, anche quelli tipicamente contrattuali [...]». Si rafforza l'impressione che il controllo attuato per esigenze di tutela del patrimonio aziendale intenda includere anche la verifica (a distanza) dell'inadempimento e dei comportamenti contrattualmente scorretti o inadeguati del lavoratore». *Contra* Nuzzo 2022.

¹³ Sulle contraddizioni dell'orientamento in parola Nogler 1998.

L'art. 4 St. lav. contiene uno scambio, poiché se, da un lato, amplia le finalità legittime di controllo diretto dell'inadempimento della prestazione lavorativa, *sub specie* di violazione degli obblighi di disciplina (art. 2104, c. 2, c.c.), dall'altro, condiziona l'utilizzabilità dei dati raccolti alla condizione che il datore abbia ricavato quella prova nel rispetto dei vincoli di trasparenza e proporzionalità. Per questa via il legislatore ha inteso ri-assorbire nel testo e nei limiti posti dall'art. 4 St. lav. l'orientamento giurisprudenziale sui controlli difensivi,

Parte della giurisprudenza di merito, accorgendosi del cambiamento, ritiene che la prova sia ammissibile quando emerga nel procedimento disciplinare e nel giudizio che il datore di lavoro: a) abbia predeterminato ed esplicitato base giuridica concreta e finalità disciplinare del controllo, prima della sua realizzazione, esplicitandole nell'accordo sindacale di cui al co. 1 quando sia previsto¹⁴; b) portato a conoscenza dei lavoratori regole di condotta per l'uso degli stessi strumenti oltreché assicurato la trasparenza sulle «modalità di effettuazione dei controlli» (art. 4, co. 3)¹⁵; c) rispettato i principi del trattamento che lo vincolano a esercitare il proprio potere secondo un canone di proporzionalità che, possa essere desunto dal funzionamento stesso dei dispositivi¹⁶.

Ciò induce a ritenere illeciti, anche penalmente, controlli continui e anelastici, non preceduti da un legittimo sospetto e dalla dimostrazione che il controllo disciplinare costituisca l'*extrema ratio* a seguito di tentativi infruttuosi di

¹⁴ È illegittimo il controllo effettuato sul computer aziendale in uso al dipendente per violazione sia della disposizione statutaria che dell'art. 11, d.lgs. n. 196 del 2003, poiché tale comportamento integra la fattispecie di trattamento dei dati personali del lavoratore effettuato all'infuori dei canoni di lealtà e correttezza e non per scopi determinati, espliciti e legittimi, Trib. Ferrara 27 agosto 2012.

¹⁵ App. Torino, 27 marzo 2017, *Il giuslavorista*, 2 agosto 2017, 15, che ha dichiarato l'inutilizzabilità delle comunicazioni Skype di un lavoratore in quanto «non risulta[va] in alcun modo che il datore di lavoro avesse preventivamente adottato e comunicato ai dipendenti un regolamento sull'uso degli strumenti informatici *hardware* e *software* forniti in dotazione dall'azienda per lo svolgimento della prestazione lavorativa, nonché sulla possibilità e sulle modalità degli eventuali controlli circa il loro utilizzo». In questi termini, anche Trib. Roma, 13 giugno 2018, n. 57668, cit. ad avviso del quale le informazioni ricavate da un controllo indiretto, eseguito per tutelare il patrimonio aziendale, «sono utilizzabili, nel rispetto delle regole sulla *privacy* e della regola specifica della previa informazione al lavoratore, «a tutti i fini connessi al rapporto di lavoro»; espressione di latitudine tale da comprendere anche il controllo sull'osservanza degli obblighi discendenti dal rapporto di lavoro». La sentenza poi dichiara inutilizzabili le informazioni raccolte per mancanza di un'«adeguata informazione». Ma si veda La Spezia 25 novembre 2016, *DRI*, 2019, 1, 302 sgg. nt. G. Cassano che dopo aver ritenuto la tessera *viacard* uno strumento di lavoro, disapplica il co. 3 dell'art. 4 St. lav.

¹⁶ Trib. Padova, 24 dicembre 2018, *NGCC*, nt. A. Ingraio, 649 che ha ritenuto legittimo il licenziamento disciplinare della dipendente di una nota compagnia telefonica che aveva eseguito diversi accessi al database contenente il registro delle chiamate delle sue utenze telefoniche. La prova della giusta causa era utilizzabile in quanto rispettato il principio di proporzionalità: il datore di lavoro aveva intrapreso misure tecniche per inibire gli accessi applicando i principi di *privacy by design* e *by default* (si trattava in specie dell'installazione di un *pop up* con funzione di *disclaimer* che al momento dell'accesso al *database* avvertiva del divieto d'accesso), anche se non aveva debitamente informato la lavoratrice.

prevenire tali illeciti attraverso misure organizzative adeguate. Il principio di responsabilizzazione, del resto, implica che le misure intraprese per prevenire il rischio di effettuare un trattamento illecito, possibilmente in collaborazione con le organizzazioni sindacali ⁽¹⁷⁾ debbano essere adeguatamente documentate.

Va nondimeno osservato che, nonostante gli apprezzabili tentativi di parte della giurisprudenza di merito di cogliere lo spirito della riforma dell'art. 4 St. lav., la giurisprudenza di Cassazione, e parte della giurisprudenza di merito, continua a ritenere valido l'orientamento sul controllo difensivo in spregio a qualsiasi garanzia prevista dalla legge, sebbene limitando il suo raggio a «condotte specifiche» precedute da un «legittimo sospetto»¹⁸.

Diametralmente opposta è la valutazione circa la possibilità di controllare l'adempimento della prestazione di lavoro, della produttività e del rendimento individuale per poi utilizzare i dati a fini disciplinari.

Benché infatti il tracciamento della prestazione sia materialmente reso possibile dalle moderne tecnologie integrate nel processo produttivo, si reputa che le esigenze organizzative e produttive non possano costituire base giuridica di un trattamento di dati con finalità disciplinare, poiché quelle esigenze riguardano l'organizzazione d'impresa nel suo complesso e non invece la produttività di ogni singolo lavoratore. Del pari, le esigenze implicite nell'art. 4, co. 2 (rendere la prestazione lavorativa e registrare gli accessi e le presenze) non legittimano tale tipo di sorveglianza.

Tale controllo, per sua natura continuativo e anelastico, costituirebbe dunque un mezzo sproporzionato per raggiungere un fine patrimoniale del datore di lavoro su cui prevale la libertà e la dignità umana del lavoratore interessato dal trattamento. Del resto in un bilanciamento costituzionalmente e imposto tra i valori in gioco, non si dubita che mettere sotto pressione la persona che lavora, inducendola a sforzi stacanovisti, sarebbe altresì contrario alla sua salute e sicurezza.

¹⁷ In coerenza con i meccanismi di consultazione sindacale previsti dalla Raccomandazione (2015)5 del Comitato dei Ministri (punto n. 15) la collaborazione sindacale potrebbe spingersi a rappresentare il veicolo di un'informazione generalizzata al gruppo di lavoratori interessati per indurre il soggetto o i soggetti sospettati a cessare il comportamento.

¹⁸ Cass. 22 settembre 2021 n. 25732: «Sono consentiti i controlli anche tecnologici posti in essere dal datore di lavoro finalizzati alla tutela di beni estranei al rapporto di lavoro o ad evitare comportamenti illeciti, in presenza di un fondato sospetto circa la commissione di un illecito, purché assicura sia assicurato un corretto bilanciamento tra l'esigenza di protezione di interessi e beni aziendali, correlate alle libertà di iniziativa economica rispetto alle imprescindibili tutela della dignità sempre che il controllo riguardi dati acquisiti successivamente all'insorgere del sospetto. 31. Occorre distinguere tra i controlli a difesa del patrimonio aziendale che riguardano tutti i dipendenti o gruppi di dipendenti nello svolgimento della loro prestazione di lavoro che li pone a contatto con il patrimonio aziendale, che dovranno essere realizzati nel rispetto dell'art. 4 novellato e controlli difensivi in senso stretto diretti ad accertare specificamente condotte illecite ascrivibili a singoli dipendenti, anche se questo si verifica durante la prestazione di lavoro. Questi ultimi si situano all'esterno dell'ambito applicativo dell'articolo 4».

L'interpretazione proposta è poi conforme al quadro sovranazionale, dove la Corte EDU¹⁹, nell'interpretare l'art. 8 CEDU, ha affermato che un simile controllo a distanza sulla prestazione lavorativa (nella specie si trattava di due professori universitari sorvegliati da un sistema di videosorveglianza in aula durante lo svolgimento delle lezioni) costituisce una notevole ingerenza nella sfera personale del prestatore e pertanto deve trovare un adeguato e specifico riscontro espresso nella legislazione nazionale dello Stato aderente alla Convenzione.

Se nel caso giudicato dalla Corte l'ordinamento giuridico montenegrino non possedeva una legge simile, si deve concludere che nemmeno l'ordinamento italiano ammetta questa forma di sorveglianza.

5. Le criticità della distinzione tra strumenti di controllo e strumenti di lavoro e di registrazione degli accessi e delle presenze tra incertezza e depotenziamento del ruolo sindacale

Alla luce delle garanzie del lavoratore desumibile dal sistema *privacy*, risulta notevolmente depotenziata la distinzione tra strumenti di video sorveglianza e di controllo (art. 4, co. 1) o strumenti «utilizzati dal lavoratore per rendere la prestazione» e «di registrazione degli accessi e delle presenze» (co. 2), che aveva destato le preoccupazioni della dottrina²⁰ circa la esenzione del datore di lavoro dal rispetto del requisito teleologico-funzionale oltre che della procedura sindacale o amministrativa, nell'ipotesi derogatoria di al co. 2.

Non si possono però sottacere le criticità che quella che fu salutata come la maggiore novità della riforma ha sollevato.

Innanzitutto, la distinzione tra strumenti di controllo e strumenti di lavoro ha dato vita più a problemi che a soluzioni. Poteva essere infatti prevedibile che non esistendo una nozione ontologica di strumento di lavoro ed essendo l'organizzazione delle dotazioni strumentali nonché degli scopi d'uso della tecnologia prerogativa del datore di lavoro liberamente esercitabile (art. 41 Cost.), la definizione casistica di quali strumenti servono al lavoratore a rendere la prestazione avrebbe dato vita ad orientamenti contrastanti e a nuova incertezza. Ed in effetti, provando a stilare un bilancio, si può dire che allo stato sono emerse una precisazione e due tesi.

La precisazione – quasi scontata e giunta con una circolare ministeriale del 2015 che ha preceduto la pubblicazione del nuovo testo dell'art. 4 St. lav. – invita ad analizzare partitamente l'*hardware* (cellulare, PC, Tablet) e i *softwares* che in esso sono installati (il GPS installato su smartphone, applicativi come WhatsApp²¹,

¹⁹ Corte EDU sentenza 28 novembre 2017, *Antovich e Mirkovich si veda Montenegro*.

²⁰ Barbieri 2017, 193; *ibidem* M.T. Carinci, *Il controllo «a distanza» sull'adempimento della prestazione di lavoro*, 54; Tullini 2017, 105.

²¹ Trib. Milano 24 ottobre 2017, n. 2757 (giud. Dossi), in *DRI*, 2019, 1, 302 sgg. nt. Cassano, che ha ritenuto inutilizzabili da parte del datore di lavoro i dati relativi a conversazioni Whatsapp estratte dallo smartphone in uso ad un lavoratore.

i file *log* di navigazione²²), cosicché la «scomposizione» in parola permetta all'interprete di valutare la presenza della funzionalità di controllo oppure il «vincolo di strumentalità con la prestazione lavorativa» per ciascun *software*, non dovendosi limitare a concentrare l'attenzione soltanto sulla scatola che lo contiene.

Pur essendo tutti concordi su questa condivisibile precisazione preliminare, la discordia è caduta sul criterio astratto considerato risolutivo per stabilire quali strumenti ricadono nella deroga del comma 2, per i quali non è più necessaria la codeterminazione sindacale o, in sua assenza, l'autorizzazione dell'Ispettorato del lavoro.

Secondo una prima tesi, lo strumento ricadrebbe nella deroga soltanto nell'ipotesi in cui sia indispensabile per svolgere le mansioni disimpegnate secondo un giudizio di necessità da effettuare caso per caso²³. Si oppone una visione più elastica di strumento di lavoro che sarebbe tale anche qualora costituisca un mero ausilio al lavoratore, facilitando, ottimizzando velocizzando l'inserimento della prestazione lavorativa nell'organizzazione datoriale o, addirittura, nell'ipotesi in cui abbia un mero ruolo attivo nell'impiego dello strumento²⁴.

²² Trib. Torino 19 settembre 2018, 1664 (giud. Filicetti) «non può ignorarsi il fatto che sia gli hardware sia i software generano file *log* che registrano informazioni riguardanti le operazioni eseguite dal lavoratore [...] è evidente che le componenti che generano file di *log* e consentono operazioni di monitoraggio e tracciatura degli accessi a Internet non possono essere considerati strumenti utilizzati dal lavoratore per rendere la prestazione». Cass. 19 settembre 2016, n. 18302, *RIDL*, 2017, II, 1, nt. A. Ingraio, *Il controllo disciplinare e la privacy del lavoratore dopo il Jobs Act*, che vietava all'Istituto Poligrafico e Zecca dello Stato l'impiego di *software* che operano in *background* come *Websense*, il quale, oltre a consentire il filtraggio della navigazione su siti non attinenti allo svolgimento dell'attività lavorativa, permetteva di registrare sistematicamente e memorizzare per un anno ogni accesso e tentativo di accesso a siti internet effettuato da ciascun lavoratore. *Websense*, inoltre, categorizzava le pagine visitate da ciascun lavoratore, raggruppandole in una molteplicità di classi predefinite (*entertainment, vehicles, marketing, sex*, etc.) per poi generare un *report* individuale. La Corte dichiarava tale dispositivo illecito perché installato in violazione dell'art. 4 St. lav. (vecchio testo) e dell'art. 8 St. lav. Cfr. altresì Garante per la protezione dei dati personali, provvedimento del 13 luglio 2016, *Trattamento di dati personali dei dipendenti mediante posta elettronica e altri strumenti di lavoro*, [doc. web n. 5408460] e Circolare Isp. Naz. Lav., 7 novembre 2016, n. 2.

²³ Per Trib. Milano 24 ottobre 2017, n. 2757, cit., *WhatsApp*, dove la lavoratrice licenziata aveva espresso critiche al datore di lavoro, non è indispensabile per svolgere le mansioni di commessa e, dunque, non essendo stato l'applicativo oggetto di codeterminazione i dati non sarebbero utilizzabili e il fatto disciplinarmente rilevante considerato insussistente. Per Trib. Torino 19 settembre 2018, 1664 nemmeno i *log* di navigazione possono considerarsi strumento di lavoro poiché non coesenziali allo svolgimento della prestazione. Per il Trib. Roma, ordinanza 13 giugno 2018 n. 57668 (giud. Conte) la posta elettronica ed un sistema gestionale della fatturazione sono strumenti di controllo perché di fatto permettono di controllare la prestazione e perciò non rientrano nella deroga di cui al comma 2.

²⁴ Tribunale La Spezia 25 novembre 2016, *DRI*, 2019, 1, 302 sgg. nt. G. Cassano secondo cui una tessera Viacard consegnata a una rappresentante commerciale in sostituzione del denaro contante è strumento di lavoro. Trib. Roma 24 marzo 2017 (giud. Bellini), ord., 24 marzo 2017, *DRI*, 2018, 1, 265 sgg., nt. E. Gramano, *La rinnovata (ed ingiustificata) vitalità della giurisprudenza in materia di controlli difensivi*. per cui è sufficiente che il lavoratore abbia un «ruolo attivo» nell'uso dello strumento.

In secondo luogo, ma non meno importante, se pur è vero che la distinzione non consente al datore di lavoro di esercitare il proprio potere in modo completamente arbitrario, essa rende difficile per la Rsa/Rsu l'ispezione e la successiva codeterminazione dell'installazione di una parte di dispositivi che incorporano funzioni di controllo. Poiché infatti la legge non sostiene più tale tipo di contrattazione, che in passato era indotta dall'obbligo a trattare di origine legale, essa tutt'al più potrà scaturire caso per caso a seconda dei mutevoli rapporti di forza dell'organizzazione sindacale nel singolo luogo di lavoro.

Si considera questa modifica la maggiore criticità del nuovo art. 4 St. lav. e perciò su tale aspetto saranno svolte alcune osservazioni conclusive e formulata una proposta per il suo superamento (*infra* par. 6).

6. Una proposta per il superamento di alcune criticità della lettura proposta: il Rappresentante dei lavoratori per la *privacy*

Rimangono da svolgere alcune considerazioni conclusive all'esito della lettura integrata tra controllo a distanza e *privacy* e si vuole incominciare dal punto più dolente dell'intero impianto che affligge sia l'art. 4 St. lav. sia il sistema a protezione dei dati personali delle persone fisiche. Nessuno dei due dà lo spazio che merita alla dimensione collettiva del problema del controllo a distanza che – come hanno ben messo in luce i primissimi studiosi della materia (Smuraglia 1960) – non è mai un problema individuale del singolo lavoratore, ma una questione «indivisibile», che necessariamente coinvolge tutti i prestatori che si trovano nel medesimo luogo d'installazione delle apparecchiature (Zoli 2010, 494).

Si è detto della scivolosa distinzione contenuta nei primi due commi dell'art. 4 St. lav. (*supra* par. 5) che riduce l'ambito degli obblighi a trattare per una indefinita parte di strumenti. A ciò si aggiunga il «peccato originale» di cui è macchiata la normativa *privacy* che nasce e si sviluppa con una forte vocazione individualistica che troppo poco spazio lascia alla dimensione collettiva-sindacale dei trattamenti di dati²⁵, la quale, invece, nell'immaginario lavoristico rappresenta un solido baluardo per la difesa e l'effettività dei diritti dei lavoratori. E seppure l'interesse sindacale si è destato con ritardo sulle questioni che avrebbero dovuto essere approcciate con una contrattazione d'anticipo o, se il sindacato in azienda se è interessato solo a strumenti di controllo macroscopici come i sistemi di videosorveglianza o alle macchine utensili a controllo numerico, ciò non significa che non siano stati siglati accordi interessanti con nuove garanzie per i lavoratori, anche dal punto di vista della protezione dei dati per-

²⁵ Per esempio, la disciplina della «valutazione d'impatto» *privacy* (art. 35 Reg.) prevede che nell'esecuzione della mappatura, il titolare-datore di lavoro «se del caso» raccoglie «le opinioni degli interessati o dei loro rappresentanti sul trattamento» che intende effettuare (art. 35,9, Reg.). Non è quindi previsto un vero e proprio dovere del datore di lavoro di sottoporre i sistemi adottati al vaglio delle rappresentanze sindacali.

sonali, giacché in alcuni accordi il flusso d'informazioni personali dei lavoratori è interamente contrattato sino alla cancellazione dei dati²⁶.

Né tantomeno si reputa che l'atteggiamento sindacale, che rivela un contegno mantenuto in epoche in cui la tecnologia non era ancora sofisticata come è oggi, debba essere il criterio guida per l'emanazione di norme lavoristiche inderogabili e protettive. Esse semmai dovrebbero rappresentare la concretizzazione del programma costituzionale di attuazione dei principi di solidarietà (art. 2 Cost.) e uguaglianza sostanziale (art. 3, co. 2) che, completando la disciplina del contratto individuale di lavoro, lo sappiano rendere «terreno su cui cresce la pianta della democrazia industriale»²⁷.

La mancanza di una norma che obblighi il datore di lavoro a confrontarsi e a coinvolgere i rappresentanti dei lavoratori, dunque, andrebbe colmata sul piano legislativo, ritornando sui passi lungimiranti dell'originario art. 4 St. lav. il quale riconosceva l'estrema importanza che in questa materia riveste la codeterminazione, così come del resto il sistema del consiglio d'Europa ha più volte affermato nelle sue raccomandazioni²⁸. Tanto più che è oramai acquisizione consolidata in dottrina che i dati non servono più soltanto a controllare, ma costituiscono il substrato informativo del potere direttivo, quando le decisioni di gestione del rapporto di lavoro sono prese dagli algoritmi²⁹.

Con una buona dose di realismo, però, occorre ammettere che tale intervento è di là da venire. Infatti, il recente D.lsg. 104/2022 cd. Decreto trasparenza (Carinci, Giudici, Perri 2023), che intendeva potenziare la trasparenza dei siste-

²⁶ Accordo Almagia Contact center e le RSU del sito di Napoli, in data 16 febbraio 2017, che seguendo una procedura di licenziamento collettivo è volto all'incremento della competitività, alla gestione della crisi e alla tutela dei livelli di occupazione nel sito. Si prevede, al fine di migliorare la qualità del servizio alla clientela e la produttività del personale, «nel rispetto di quanto previsto dall'art. 4 St. lav.» che il singolo operatore sia assoggettato alla misurazione quantitativa e qualitativa della prestazione «allo scopo di individuare eventuali aree di miglioramento, mediante lo svolgimento di precorsi formativi propedeutici all'allineamento agli standard di efficienza e qualità richiesti dalla commessa». Si prevedono poi nell'accordo diverse garanzie: innanzitutto i dati di risultato tracciati sono comunicati al singolo lavoratore controllato, mentre, soltanto per la quota del 60%, sono visibili ad una figura di *staff* che svolge funzioni di miglioramento delle *performance*. Il responsabile gerarchico diretto, invece, non ha mai accesso a tali dati. Si prevede, inoltre, che i dati ricavati non possono essere utilizzati a fini disciplinari e nemmeno per definire avanzamenti di carriera. Infine, si assicura il rispetto delle norme del codice della *privacy*, del tempo di conservazione dei dati. Per l'analisi di altri casi e accordi aziendali sia consentito rinviare a Ingrao 2019 e Bellavista 2014.

²⁷ Veneziani 1987, spec. 35; Pedrazzoli 1985; Smuraglia 1960, spec. 311-316, il quale, facendo leva sul precepto dell'art. 46 Cost. ipotizzava, prima dell'emanazione dello Statuto dei lavoratori, che i lavoratori per il tramite delle associazioni collettive potessero «studiare con la direzione aziendale i problemi» che dall'installazione di impianti di videosorveglianza potessero derivare e, una volta installate le telecamere, controllarne l'uso.

²⁸ Rivestono solo una funzione d'orientamento dell'interpretazione normativa i principi d'informazione e consultazione posti dall'art. 21 della Raccomandazione del Comitato dei Ministri del Consiglio d'Europa R(2015)5 del 1 aprile 2015.

²⁹ Per tutti si veda Zappalà 2021.

mi di monitoraggio e di decisione automatizzata – gli algoritmi decidenti – non è riuscito a cogliere l’occasione per inserire accanto al diritto informativo della Rsu un obbligo di consultazione sindacale in questa materia.

Per tale ragione, si è già avuto modo di proporre e discutere con alcune federazioni di categoria particolarmente toccate dal tema della digitalizzazione e del rafforzamento dei poteri di controllo (e direzione) della istituzione per via contrattuale a livello di categoria, ma anche aziendale, di una figura di rappresentanza specifica, il rappresentante dei lavoratori per la privacy. In assenza di una specifica presa di posizione del legislatore, la contrattazione collettiva potrebbe sopperire prevedendo una forma specializzata e debitamente formata di rappresentanza dei lavoratori sulla falsariga del Rappresentante dei lavoratori per la sicurezza da includere all’interno della Rsu, non solo a causa della sua legittimazione contrattuale, ma anche in ragione di una tendenza più ampia della contrattazione collettiva a razionalizzare le figure di rappresentanza accentrando le funzioni in unico organo³⁰. Poiché la prevenzione del rischio da trattamento illecito è un obbligo che deriva dal regime di responsabilizzazione del titolare del trattamento (*supra* par. 3) anche il datore di lavoro avrà interesse all’istituzione di una simile figura che funga di anello di collegamento tra i lavoratori interessati dai trattamenti e il vertice dell’organizzazione aziendale che predispose le misure atte ad umanizzare la tecnologia e a renderla rispettosa dei diritti. Non è un caso, infatti, che la logica prevenzionistica di matrice comunitaria accomuni le normative: il modello da costruire è quello della prevenzione partecipata.

Ci si propone in un futuro studio dedicato a tale tematica di analizzare e studiare le prerogative sindacali che il RLP potrebbe assumere. Mi limito qui a osservare che il RLP dovrebbe potere intervenire a monte del consolidamento delle strategie di protezione, ossia nella fase iniziale del processo di prevenzione che coincide con la mappatura dell’organizzazione tecnologica. La contrattazione collettiva dovrebbe prevedere un obbligo di consultazione preventiva e tempestiva del RLP in ordine alla valutazione dei rischi da trattamento di dati nonché alla individuazione, programmazione, realizzazione e verifica delle misure di prevenzione del rischio in azienda o nella unità produttiva.

A tal fine questa figura dovrebbe essere resa destinataria di tutte le informazioni che riguardano i sistemi informatici e rimanere aggiornata sui nuovi settaggi dei dispositivi che raccolgono e utilizzano dati dei lavoratori o che comunque incidono sui margini di autonomia di questi nell’esecuzione del lavoro; il dovere d’informazione del datore di lavoro alla Rsu/Rsa (O in loro assenza alle sedi territoriali delle associazioni sindacali comparativamente più rappresentative sul piano nazionale) è già peraltro previsto dall’art. 1bis d.lgs. 26 maggio 1997, n. 152, introdotto dal cd. Decreto trasparenza.

³⁰ Sulla razionalizzazione delle figure rappresentative si dovrebbe seguire il modello degli accordi interconfederali sulla rappresentanza, in particolare si veda il punto 2.3.1. dell’Allegato al Patto per la Fabbrica. Analoghe considerazioni circa il rappresentante dei lavoratori per la sicurezza e l’ambiente (RLSA) in Tomassetti 2021, spec. 169.

Infine, è importante, al fine di rafforzare i poteri informativi del RLP, che questa figura non soltanto riceva una formazione adeguata in termini di alfabetizzazione digitale, ma che altresì resti in collegamento costante con il DPO, il cd. *Data Protection Officer* che – ove sia nominato – costituisce, nella logica regolamentare, un sostituto del Garante all'interno dell'organizzazione, dovendo sovrintendere a qualsiasi trattamento e verificarne la conformità rispetto alla normativa.

Riferimenti bibliografici

- Barbieri, M. 2017. "L'utilizzabilità delle informazioni raccolte: il Grande Fratello può attendere (forse)." In *Controlli a distanza e tutela dei dati personali del lavoratore*, a cura di P. Tullini, 183-208. Torino: Giappichelli.
- Bellavista, A. 2007. "La disciplina della protezione dei dati personali e i rapporti di lavoro." In *Diritto del lavoro. Commentario*, a cura di C. Cester, II ed., 479 sgg. Torino: Utet.
- Bellavista, A. 2014. "Gli accordi sindacali in materia di controlli a distanza sui lavoratori." *LG* 8-9: 737 sgg.
- Bellavista, A. 2022. "Controlli tecnologici e privacy del lavoratore." In *Tecnologie digitali, poteri datoriali e diritti dei lavoratori*, a cura di A. Bellavista e R. Santucci, 99 sgg. Torino: Giappichelli.
- Carinci, M. T., Giudici, S., Perri, P. 2023. "Obblighi di informazioni e sistemi decisionali e di monitoraggio automatizzati (art. 1-bis «Decreto Trasparenza»): quali forme di controllo per i poteri datoriali algoritmici?" *Labor*, 5 sgg.
- Carnelutti, F. 1955. "Il diritto alla vita privata." *RTDPub*, 3 sgg.
- Chico, P. 2000. *Privacy e lavoro. La disciplina del trattamento di dati personali del lavoratore*. Bari: Cacucci.
- De Cupis, A. 1959. *Teoria generale, diritto alla vita e all'integrità fisica, diritto sulle parti staccate del corpo e sul cadavere, diritto alla libertà, diritto all'onore e alla riservatezza*. Milano: Giuffrè.
- Del Punta, R. 2016. "La nuova disciplina dei controlli a distanza sul lavoro (art. 23, d.lgs. 151/2015)." *RIDL* I: 77 sgg.
- Dessi, O. 2018. *Il controllo a distanza sui lavoratori*. Napoli: Esi.
- Friedman, W. H. 2000. "Is the answer to Internet addiction, Internet interdiction?" In *Proceedings of the 2000 Americas Conference on Information Systems*, a cura di M. Chung.
- Gamba, C. 2016. "Il controllo «a distanza» delle attività dei lavoratori e l'utilizzabilità delle prove." *LLI* 2, 1: 122 sgg.
- Ingrao, A. 2018. *Il controllo a distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata*. Bari: Cacucci.
- Ingrao, A. 2019. "Data-Driven management e strategie collettive di coinvolgimento dei lavoratori per la tutela della privacy." *LLI* 5, 2: 127 sgg.
- Lener, A. 1985. "Voce Potere (dir. priv.)." In *ED*, vol. XXXIV, 635 sgg. Milano: Giuffrè.
- Marazza, M. 2016. "Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore)." *WP CSDLE «Massimo D'Antona»* 300: 25 sgg.
- Maresca, A. 2017. "Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 St. lav." In *Controlli a distanza e tutela dei dati personali del lavoratore*, a cura di P. Tullini. Torino: Giappichelli.

- Nogler, L. 1998. "Sulle contraddizioni logiche della Cassazione in tema di diritto alla riservatezza del lavoratore subordinato." *RCP* 1: 113 sgg.
- Nuzzo, V. 2018. *La protezione del lavoratore dai controlli impersonali*. Napoli: Editoriale Scientifica.
- Nuzzo, V. 2018. *La protezione del lavoratore dai controlli impersonali*. Napoli: Editoriale Scientifica.
- Pedrazzoli, M. 1985. *Democrazia industriale e subordinazione. Poteri e fattispecie nel sistema giuridico del lavoro*. Milano: Giuffrè.
- Pisani, C., Proia, G., Topo, A. 2022. *Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro*. Milano: Giuffrè.
- Proia, G. 2016. "Trattamento dei dati personali, rapporto di lavoro e l'«impatto» della nuova disciplina dei controlli a distanza." *RIDL* 1, 4: 560 sgg.
- Rodotà, S. 1997. "Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali." *RCDP*, 698 ssg.
- Sartori, A. 2020. *Il controllo tecnologico sui lavoratori. La nuova disciplina italiana tra vincoli sovranazionali e modelli comparati*. Milano: Giuffrè.
- Sitzia, A. 2016. "Il controllo (del datore di lavoro) sull'attività dei lavoratori: il nuovo articolo 4 St. lav. e il consenso (del lavoratore)." *LLI* 2, 1: 83 sgg.
- Smuraglia, C. 1960. "Progresso tecnico e tutela della personalità del lavoratore (a proposito dell'installazione di impianti di ripresa televisiva nelle fabbriche)." *RGL* I: 303-16.
- Tomassetti, P. 2021. "Ambiente di lavoro e di vita: fonti regolative e standard di prevenzione." *RGL*.
- Tullini, P. (a cura di). 2017. *Controlli a distanza e tutela dei dati personali del lavoratore*. Torino: Giappichelli.
- Tullini, P. 2017. "Il controllo a distanza attraverso gli strumenti per rendere la prestazione lavorativa. Tecnologie di controllo e tecnologie di lavoro: una distinzione è possibile?" In *Controlli a distanza e tutela dei dati personali del lavoratore*, a cura di P. Tullini, 97 sgg. Torino: Giappichelli.
- Veneziani, B. 1987. "Nuove tecnologie contratto di lavoro: profili di diritto comparato." *DRLI* 1, 33.
- Zappalà, L. 2021. "Informatizzazione dei processi decisionali e diritto del lavoro: algoritmi, poteri datoriali e responsabilità del prestatore nell'era dell'intelligenza artificiale." *Biblioteca 20 maggio* 2: 98 sgg.
- Zoli, C. 2010. "Contratto collettivo come fonte e contrattazione collettiva come sistema di produzione di regole." In *Trattato di diritto del lavoro*, vol. 1, a cura di M. Persiani e F. Carinci. Padova: Cedam.