# UNIVERSITÀ DEGLI STUDI DI PADOVA

DIPARTIMENTO DI DIRITTO PRIVATO E CRITICA DEL DIRITTO



CORSO DI LAUREA IN CONSULENTE DEL LAVORO

A.A. 2022 – 2023

# I DIRITTI DEI LAVORATORI E IL POTERE DI CONTROLLO NELL'INDUSTRIA 4.0.


Relatrice

Prof.ssa Silvia Bertocco

Studentessa

Raffaella Adami

# INDICE

# INTRODUZIONE

Industria 4.0 integra alcune nuove tecnologie produttive per migliorare le condizioni di lavoro e aumentare la produttività e la qualità degli impianti; l'obiettivo è giungere alla produzione industriale del tutto automatizzata e interconnessa.

Il termine Industria 4.0 è stato utilizzato la prima volta alla Fiera di Hannover del 2011; nell'edizione 2013 è stato presentato il report del gruppo di lavoro costituito in Germania per l'elaborazione del piano industriale del governo tedesco, per ammodernare il sistema produttivo e renderlo competitivo a livello globale.

Finora si contavano tre rivoluzioni industriali. La prima a partire dal 1784, con la nascita della macchina a vapore e la conseguente meccanizzazione della produzione, la seconda a partire dal 1870 con l'inizio della produzione di massa, attraverso l'utilizzo dell'elettricità, del motore a scoppio e dei derivati del petrolio, la terza dal 1970 con l'avvento dei Personal Computer e l'introduzione dei sistemi elettronici e dell'informatica.

Le nuove tecnologie digitali rappresentano il cuore della quarta rivoluzione industriale, definita anche Industria 4.0, e avranno un impatto profondo sul processo produttivo e sull'organizzazione del lavoro.

Gli sviluppi possibili sono molteplici, a partire dall'utilizzo dei dati, la potenza di calcolo e la connettività che si declina in Big data[1], Open data, Internet of Things, machine to machine e cloud computing per la centralizzazione delle

[1] Nel 2001 Doug Laney (in 3D Data Management: controlling data Volume, Velocity and Variety, Meta Groups Report) descrisse i Big data con il modello delle 3V: Volume, Velocità e Varietà; a tale paradigma gli esperti hanno successivamente aggiunto Veridicità e Variabilità e oggi si parla per i Big Data di Modello delle 5V

informazioni e la loro conservazione.

Fondamentale si rivela la Data Analytics, che mira a ricavare valore dal[2]l'enorme quantità di dati resi disponibili attraverso processi di machine learning e di costumers analysis, che perseguono la finalità di orientare la produzione in base alle esigenze e preferenze dei consumatori.

Altre direttrici di sviluppo sono realizzate attraverso l'interazione tra uomo e macchina, che coinvolge le interfacce "touch", sempre più diffuse, e la realtà aumentata.

Infine, si ricorda lo sviluppo del settore che si occupa del passaggio dal digitale al reale, e che comprende la manifattura additiva, la stampa in 3D, la robotica, le comunicazioni, le interazioni machine to machine e le nuove tecnologie per immagazzinare e utilizzare l'energia in modo mirato, razionalizzando i costi e ottimizzando le prestazioni.

Esperti e osservatori stanno cercando di comprendere le linee evolutive del mondo del lavoro, quali nuove professionalità saranno necessarie e quali invece presto potrebbero scomparire, quali competenze e abilità saranno richieste ai lavoratori del futuro, così da poter cogliere appieno i benefici della Quarta rivoluzione industriale, attuando iniziative sistemiche per lo sviluppo della Smart Manifacturing e fornendo ai lavoratori le competenze richieste per le professioni del futuro.

In tal senso il governo italiano ha previsto, a partire dal piano del governo per l'Industria 4.0 contenuto della legge di bilancio 2017, una serie di interventi per incentivare le imprese ad adeguarsi e ad aderire pienamente alla Quarta rivoluzione. L'osservatorio Industria 4.0 del Politecnico di Milano definisce le soluzioni di digitalizzazione dei processi di produzione e supply chain: manifacturing Big Data, Additive Manufacturing (stampa 3D), Industrial

Internet of Things, Cloud, Advanced Automation e Advanced HMI (Human Machine Interface).

Il piano nazionale Industria 4.0 non è solo funzionale al rinnovamento delle infrastrutture produttive (beni strumentali, impianti, hardware e software per le industrie) ma ha anche l'obiettivo di costruire un nuovo modo di organizzare il lavoro.

La digitalizzazione interessa non solo il campo della produzione con l'introduzione di nuovi macchinari e tecnologie, ma anche quello dell'organizzazione del lavoro e dell'HR management, con modifiche che attengono anche ai luoghi e alle modalità di effettuazione della prestazione.

Due sono gli elementi della nuova rivoluzione industriale che incidono direttamente sui diritti dei lavoratori: la velocità e l'ubiquità.

L'algoritmo e le macchine intelligenti offrono un valore aggiunto nell'ambito del sistema produttivo globale proprio attraverso la velocità, che crea efficienza e cadenza lo svolgimento del lavoro, creando un nuovo modo di organizzare il contesto aziendale basato sull'interfaccia tra persona e macchina nell'organizzazione della produzione.

Per quanto riguarda l'ubiquità del posto di lavoro, basti solo pensare all'ausilio delle nuove tecnologie digitali, che velocizzano ogni attività umana; l'ufficio ora è potenzialmente ovunque.

Luogo e tempo di lavoro assumono quindi una dimensione del tutto nuova, completamente diversa da quella conosciuta finora e basata sulla presenza fisica in azienda.

L'Industria 4.0, figlia della digitalizzazione, dell'Intelligenza Artificiale e dell'algoritmo, richiede quindi ai lavoratori nuove competenze e sempre maggiore adattabilità; importanza fondamentale assume a questo proposito la necessità continua di formazione e di aggiornamento, non solo delle

competenze tecniche ma anche delle capacità di relazione, le cosiddette soft skills.

Come sempre è accaduto e accade in presenza di processi evolutivi dirompenti per l'economia e la società, ci troviamo di fronte a grandi opportunità ma anche a notevoli rischi, in particolare per i lavoratori e i loro diritti.

Partendo dall'analisi del quadro normativo di riferimento del diritto del lavoro, è possibile verificare come impattano le nuove tecnologie sulla tutela dei diritti e quali strategie si stanno realizzando a livello europeo e nazionale per far fronte alle modifiche degli assetti tradizionali nel mondo del lavoro.

# CAPITOLO 1

# LE NUOVE TECNOLOGIE

## 1.1 Le nuove tecnologie

A partire dagli anni Ottanta del secolo scorso abbiamo assistito a una serie di cambiamenti nei mezzi di comunicazione e nella strumentazione utilizzata nei luoghi di lavoro, che hanno completamente rivoluzionato il modo di lavorare e di comunicare.

In questo capitolo illustreremo i nuovi strumenti e le nuove tecniche di comunicazione, analizzando le ricadute che il loro utilizzo può avere per l'instaurazione e lo svolgimento del rapporto di lavoro.

## 1.2. La comunicazione via mail e la messaggistica via web

La comunicazione epistolare in questi ultimi decenni è stata quasi completamente sostituita dalla posta elettronica, che consente di trasmettere informazioni e ricevere risposte in tempi estremamente ridotti rispetto al passato, e a costi decisamente contenuti.

I datori di lavoro possono mettere a disposizione dei loro dipendenti uno strumento di comunicazione efficace e veloce, da utilizzare sia per inviare messaggi all'esterno sia per comunicare con i colleghi all'interno dell'azienda.

Al pari della corrispondenza epistolare, anche la posta elettronica è tutelata dal diritto alla segretezza della corrispondenza previsto dall'articolo 15 della Costituzione, e sono applicabili le regole sul divieto di indagine da parte dei datori di lavoro sui contenuti delle comunicazioni.

Alle mail si sono aggiunte in questi ultimi anni altre forme di comunicazione e anche i datori di lavoro sempre più utilizzano blog aziendali, community di

dipendenti, gruppi whatsapp o altre applicazioni simili per mettere in contatto i dipendenti tra di loro a basso costo e con strumenti sempre accessibili a tutti. Se queste tecnologie rappresentano un'opportunità notevole per creare connessioni, trasmettere e ricevere informazioni da e tra i dipendenti in modo fluido e soprattutto immediato, per contro esse aumentano il rischio che siano utilizzate in modo poco opportuno, diventando veicolo di acquisizione di informazioni strettamente personali che non sempre il datore di lavoro o i colleghi sono tenuti a trattare, in ossequio al divieto di indagine di cui all'art. 8 St. Lav.[3]

Il corretto utilizzo di tali strumenti è quindi condizione imprescindibile per il rispetto dei diritti dei lavoratori.

A tal proposito assumono estrema rilevanza le *Linee guida del Garante per l'utilizzo della posta elettronica e di internet del 01/03/2007*, documento n. 1387522.[4]

Il Garante prescrive ai datori di lavoro l'adozione di alcune misure necessarie od opportune per garantire il rispetto della normativa, muovendo da alcune premesse. Innanzitutto, spetta al datore di lavoro il compito di assicurare la funzionalità e il corretto impiego degli strumenti digitali da parte dei lavoratori, definendone le modalità d'uso nell'organizzazione dell'attività lavorativa e adottando misure di sicurezza idonee. Il Garante sottolinea poi l'evoluzione delle tecnologie e i rischi connessi al loro utilizzo, che con il progresso sono costantemente in aumento, come ad esempio la difficoltà di stabilire la linea di confine tra l'attività lavorativa e la vita privata del lavoratore poiché il luogo di lavoro è una formazione sociale nella quale il

[3] V. Pinto, *I controlli difensivi del datore di lavoro sulle attività informatiche e telematiche del lavoratore*, in P. Tullini (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Giappichelli Editore, 2017, p. 152

[4] G. Finocchiaro, *Limiti posti dal Codice in materia di protezione die dati personali al controllo del datore id lavoro*, in P. Tullini (a cura di), *Web e lavoro. Profili evolutivi e di tutela*, Giappichelli editore, 2017, pag. 57

lavoratore può esplicare la propria personalità, e in tal senso vanno quindi garantiti i suoi diritti.

L'utilizzo della posta elettronica nel contesto lavorativo, anche in ragione della veste esteriore attribuita all'indirizzo mail nei singoli casi, può generare il dubbio che il lavoratore, in qualità di destinatario o mittente, utilizzi la posta elettronica operando per conto dell'azienda oppure ne faccia un uso personale. Secondo il Garante[5], l*a mancata esplicitazione di una policy al riguardo può determinare anche una legittima aspettativa del lavoratore, o di terzi, di confidenzialità rispetto ad alcune forme di comunicazione;* questo può generare incertezze e costituire un vincolo per il datore di lavoro che intenda apprendere il contenuto di messaggi inviati all'indirizzo di posta elettronica usato dal lavoratore.

L'autorità garante prescrive quindi una serie di misure che i datori di lavoro sono tenuti a porre in essere, in particolare l´onere di specificare le modalità di utilizzo della posta elettronica da parte dei lavoratori, con la chiara indicazione delle modalità d'uso degli strumenti messi a disposizione e dell'effettuazione di eventuali controlli; indica poi una serie di raccomandazioni a carattere organizzativo e tecnologico, tra le quali spicca l'adozione e la pubblicizzazione di un disciplinare interno e misure di carattere organizzativo e tecnologico riferite ad esempio alle postazioni lavorative, all'utilizzo di indirizzi mail condivisi eventualmente affiancati a indirizzi individuali, all'attribuzione se possibile ai lavoratori di un ulteriore indirizzo di posta utilizzabile per le comunicazioni personali e alcune misure da porre in essere in caso di assenza improvvisa o prolungata del lavoratore per verificare il contenuto dei messaggi strettamente necessari all'attività

[5] *Linee guida per la posta elettronica e internet*, 1° marzo 2007, doc. web n. 1387522, in www.garanteprivacy.it

lavorativa.

Nelle Linee Guida viene, inoltre, esplicitata la possibilità di effettuare controlli a distanza e di trattare dati personali non sensibili per perseguire un interesse legittimo del datore di lavoro nel rispetto delle norme in materia; peraltro, tale possibilità risulta bilanciata dal divieto di leggere e registrare sistematicamente i messaggi di posta elettronica o i relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail.

Nonostante la presenza di disposizioni specifiche resta cruciale la difficile distinzione tra sfera lavorativa e sfera personale, che può provocare nell'utilizzo della posta elettronica notevoli problemi di liceità del trattamento.

## 1.3. L'accesso a internet

Il mondo del lavoro è sempre più interconnesso e l'accesso a internet è ormai diventato uno strumento indispensabile per la maggior parte dei lavoratori, funzionale all'utilizzo della posta elettronica e degli altri strumenti di comunicazione ma anche per lo svolgimento della stessa attività lavorativa, che si esplica sempre più attraverso il collegamento a siti istituzionali e privati.

Anche in questo caso la tecnologia rappresenta una notevole opportunità ma nasconde anche alcuni rischi, sia per il datore di lavoro che per il lavoratore.[6]

Il datore di lavoro, nel consegnare al dipendente uno strumento di tale portata, potrà legittimamente temere che non sia utilizzato soltanto per finalità aziendali e che il lavoratore durante l'orario di lavoro navighi sul web non soltanto per svolgere la propria attività ma anche per motivi personali; il rischio prospettato è che tale navigazione possa rappresentare motivo di distrazione aumentando il margine di errore, oppure che sottragga tempo alla

[6] C. Colapietro, *Digitalizzazione del lavoro e tutela della riservatezza della persona*, in P. Tullini (a cura di), *Web e lavoro. Profili evolutivi e di tutela*, op. cit., pag. 25-26

prestazione lavorativa o, nel peggiore dei casi, che rechi un pregiudizio al patrimonio aziendale attraverso la perdita o il trafugamento di dati. Infatti, la navigazione incontrollata e il download da siti non affidabili può causare l'infiltrazione di files infettati da virus informatici, con il rischio di causare notevoli danni ai beni aziendali.[7]

Se tali rischi mettono il datore di lavoro nelle condizioni di ritenere opportuno un controllo dell'attività di navigazione del lavoratore, possibile tramite l'utilizzo della cronologia dei files log[8], tale controllo potrebbe contrastare con il divieto di indagine sulle opinioni dei lavoratori previsto all'articolo 8 dello Statuto dei lavoratori: dall'elenco dei siti visitati si potrebbero infatti dedurre facilmente informazioni relative alle opinioni politiche e sindacali, al credo religioso, all'orientamento sessuale o altre opinioni personali.[9]

A tal proposito richiamiamo le già citate Linee guida del Garante per l'utilizzo della posta elettronica e di Internet del 2007, che contengono alcune specifiche misure da mettere in atto da parte del datore di lavoro per consentire il corretto utilizzo nella navigazione in Internet: l'individuazione di categorie di siti considerati correlati o non correlati con la prestazione lavorativa; la configurazione di sistemi o l´utilizzo di filtri che prevengano determinate operazioni; il trattamento di dati in forma anonima o tale da precludere l´immediata identificazione degli utenti mediante opportune aggregazioni; l´eventuale conservazione di dati per il tempo strettamente limitato al perseguimento di finalità organizzative, produttive e di sicurezza; la graduazione dei controlli.

---

[7] V. Pinto, op. cit, p. 154

[8] I files log contengono le informazioni relative alle operazioni eseguite dall'utente ad ogni accesso

[9] E. Barraco, *Privacy del lavoratore e controlli tecnologici*, Diritto e Pratica del Lavoro, 40/2016, pag. 2348

## 1.4. Telefoni cellulari, smartphone e tablet

L'utilizzo di smartphone e tablet per rendere la prestazione lavorativa è ormai la quotidiana normalità per un numero sempre crescente di lavoratori.

Le comunicazioni telefoniche possono essere sottoposte a controllo solo con provvedimento del giudice (articoli 617 e 617 bis del Codice penale) e la loro registrazione costituirebbe un illecito da parte del datore di lavoro; per finalità legate a legittime esigenze organizzative e di tutela del patrimonio aziendale, quale ad esempio il monitoraggio dei costi del traffico telefonico per l'azienda, è tuttavia permessa la registrazione del numero di chiamate e della data e ora di effettuazione.[10]

In ogni caso, poiché il sistema di controllo è idoneo a realizzare un potenziale e indiretto controllo a distanza sull'attività dei dipendenti, dovrà essere stipulato uno specifico accordo sindacale e dovrà essere fornita una specifica informativa, nel rispetto di quanto previsto dall'articolo 4 dello Statuto.

Nel caso di telefono aziendale è sempre più diffuso l'uso promiscuo, cioè quando il datore di lavoro mette a disposizione del lavoratore uno strumento che può essere legittimamente utilizzato anche per uso personale; in tale caso, per evitare i rischi per la riservatezza la tecnologia consente di associare ai numeri personali uno specifico codice, che permette di creare un doppio canale di comunicazione ed escludere così dal controllo le chiamate personali.

Fondamentale anche in tal caso è la predisposizione di un disciplinare interno, che definisca le modalità di utilizzo consentite e le indicazioni relative al trattamento e conservazione di dati ricavabili con le relative finalità,[11] da comunicare ai dipendenti interessati in modo chiaro e intellegibile.

Naturalmente per tali strumenti, utilizzati e utilizzabili non solo per le

[10] P. Rausei, *Controllo a distanza: installazione e uso dei sistemi di geolocalizzazione*, Diritto & Pratica del lavoro, Wolters Kluwer Italia srl, n. 1/2017, pag. 11-12

[11] Vedi provvedimento del Garante 11 gennaio 2018 n. 7554790

conversazioni telefoniche ma per una molteplicità di prestazioni, vale quanto detto per l'accesso ad internet e alla posta elettronica, nonché per i rischi dell'utilizzo della tecnologia GPS.

## 1.5. I sistemi di geolocalizzazione

Inizialmente la tecnologia GPS (acronimo di Global Positioning System) era utilizzata dai datori di lavoro quasi esclusivamente tramite l'installazione a bordo dei veicoli impiegati per la fornitura di servizi di trasporto di persone o cose, nonché per dare esecuzione ad ulteriori prestazioni.

Tali strumenti hanno la funzione di rintracciare o monitore l'ubicazione dei veicoli aziendali, ma il loro utilizzo improprio può generare la possibilità di localizzare la posizione dei lavoratori assegnatari dei veicoli medesimi, monitorando l'ubicazione e il comportamento degli autisti durante l'attività lavorativa.[12]

Nel provvedimento emanato in materia[13], il Garante ha ritenuto ammissibile l'utilizzo di tali tecnologie, purché sia preordinato a soddisfare esigenze organizzative e produttive ovvero per la sicurezza sul lavoro e senza che sia necessario acquisire il consenso dell'interessato, a condizione che sia data attuazione alla previsione di cui all´art. 4, L. n. 300/1970.

Sul punto, in riferimento all'applicazione delle disposizioni del novellato articolo 4 dello Statuto dei lavoratori è intervenuto anche l'Ispettorato nazionale del lavoro con la circolare n. 2 del 7 novembre 2016, stabilendo che i sistemi di geolocalizzazione, applicati agli automezzi ma anche a strumenti quali smartphone, tablet a altri dispositivi IoT[14], si possono ritenere in linea di

[12] P. Rausei, op. cit., pag. 16

[13] Garante privacy, *Sistemi di localizzazione dei veicoli nell'ambito del rapporto di lavoro - 4 ottobre 2011*, doc. 1850581

[14] Con l'acronimo IOT (Intenet of Things), si definisce una serie di tecnologie che consentono

massima e in termini generali *"un elemento "aggiunto" agli strumenti di lavoro, non utilizzati in via primaria ed essenziale per l'esecuzione dell'attività lavorativa ma per rispondere ad esigenze ulteriori di carattere assicurativo, organizzativo, produttivo o per garantire la sicurezza del lavoro";* ne consegue quindi l'applicazione del comma 1 dell'art. 4 della Legge n. 300/1970.

La circolare riconosce anche che in casi del tutto particolari, ad esempio se i sistemi di localizzazione siano installati per consentire la concreta ed effettiva attuazione della prestazione lavorativa che non potrebbe essere resa senza ricorrere all'uso di tali strumenti, oppure sia richiesta da specifiche normative di carattere legislativo o regolamentare, *"si può ritenere che gli stessi finiscano per "trasformarsi" in veri e propri strumenti di lavoro e pertanto si possa prescindere, ai sensi di cui al comma 2 dell'art. 4 della L. n. 300/1970, sia dall'intervento della contrattazione collettiva che dal procedimento amministrativo di carattere autorizzativo previsti dalla legge."*

Il citato provvedimento del Garante prevede però anche alcune prescrizioni specifiche[15] in relazione al divieto di effettuare un monitoraggio continuativo della posizione del veicolo, prediligendo un controllo solo se necessario per il conseguimento delle finalità legittimamente perseguite; nel rispetto del principio di pertinenza e non eccedenza, i tempi di conservazione dei dati dovranno essere commisurati alle finalità in concreto perseguite; ai lavoratori dovrà essere fornita l'informativa prescritta dal Codice Privacy e deve risultare chiaramente che il veicolo è soggetto a localizzazione, tramite l'utilizzo di apposite vetrofanie che rendano edotti gli interessati dell'installazione della tecnologia sul veicolo.

---

di rendere smart una serie di oggetti anche di uso quotidiano, attraverso il collegamento alla rete internet

[15] L. Califano, *Tecnologie di controllo del lavoro, diritto alla riservatezza*, in P. Tullini, *Controlli a distanza e tutela dei dati personali del lavoratore*, op. cit., pag. 176

Il trattamento dei dati di localizzazione, inoltre, deve formare oggetto di notificazione al Garante[16] e i trattamenti di dati di localizzazione che possono presentare rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità di interessati diversi dai lavoratori, possono essere sottoposti a verifica preliminare ai sensi dell'art. 17, comma 2 del Codice.

Il progresso e la diffusione delle nuove tecnologie estende ora la possibilità di caricare facilmente sistemi di localizzazione anche su dispositivi di uso quotidiano che il lavoratore porta con sé, quali smartphone o tablet, estendendo il rischio di monitoraggio costante dei lavoratori a tutti coloro che si servono di tali dispositivi quali strumenti di lavoro.[17]

Il Garante in tal senso sottolinea[18] che i dispositivi smartphone, "*in considerazione delle normali potenzialità d'uso e dell'utilizzo comune degli stessi, destinati a "seguire" la persona che li detiene indipendentemente dalla distinzione tra tempo di lavoro e tempo di non lavoro*", e il trattamento dei dati relativi alla loro geolocalizzazione "*presenta rischi specifici per la libertà, i diritti e la dignità del dipendente.*"

In relazione a tale peculiari rischi per i lavoratori, il provvedimento citato ritiene legittimo il trattamento dei dati personali dei dipendenti relativi alla localizzazione attraverso l'utilizzo dello smartphone, in applicazione della disciplina del cosiddetto bilanciamento di interessi; tuttavia, impone ai datori di lavoro alcune prescrizioni aggiuntive finalizzate a garantire il rispetto dei diritti dei lavoratori. A tal proposito la società dovrà impedire l´eventuale

---

[16] Vedi art. 37del Codice Privacy: "Il titolare notifica al Garante il trattamento di dati personali cui intende procedere, solo se il trattamento riguarda: a) dati genetici, biometrici o dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica.

[17] P. Tullini, *Il controllo a distanza attraverso gli strumenti per rendere la prestazione lavorativa*, in P. Tullini (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, op. cit, pag. 109

[18] *Trattamento di dati personali effettuato attraverso la localizzazione di dispositivi smartphone - 18 maggio 2016*, doc. 5217175, in www.garanteprivacy.it

trattamento di dati ultronei rispetto alle finalità indicate (es. dati relativi al traffico telefonico, agli sms, alla posta elettronica, alla navigazione in Internet o altro) configurando il sistema in modo da consentire il trattamento dei dati di localizzazione nei casi predeterminati; il sistema dovrà prevedere sullo schermo del dispositivo, anche quando l'applicazione lavora in background, la presenza di un´icona che indichi che la funzionalità di localizzazione è attiva.

Il Garante richiama poi il rispetto delle prescrizioni e raccomandazioni contenute nel provvedimento del Garante del 1° marzo 2007, n. 13 ("Linee guida per posta elettronica e internet"), nonché della necessità di effettuare la notificazione al Garante ai sensi dell'articolo 37 del Codice Privacy e di fornire ai dipendenti un'informativa completa.

L'analisi dei provvedimenti citati è esemplificativa del ruolo fondamentale svolto dal Garante per la corretta applicazione della normativa in materia e per il rispetto della dignità dei lavoratori.

## 1.6. La rilevazione degli accessi e l'utilizzo di tesserini magnetici

I tesserini magnetici sono utilizzati dai datori di lavoro per monitorare gli accessi dei dipendenti al luogo di lavoro ed eventuali spostamenti all'interno dell'attività produttiva. Essi permettono anche di rilevare l'utilizzo di servizi messi a disposizione dei dipendenti, come ad esempio il servizio mensa.

In relazione al loro utilizzo, il testo originale dell'articolo 4 dello Statuto dei lavoratori aveva generato un'incertezza interpretativa che trovava una prevalente interpretazione volta a legittimare l'uso del badge in assenza dei limiti previsti dall'art. 4. L'accento della dottrina era posto sul fatto che la mera rilevazione della presenza sul luogo di lavoro non integrava un controllo sull'attività del lavoratore, quindi non soggetto alle disposizioni previste

all'articolo 4 comma 2.[19]

Con la sua riforma, il legislatore ha tentato di superare i dubbi interpretativi escludendo gli strumenti di rilevazione degli accessi e delle presenze dalla procedura di autorizzazione sindacale o amministrativa.

Dunque, il legislatore sembrava aver risolto la criticità senza però considerare, come ha immediatamente sottolineato parte della dottrina, la possibilità che i dati registrati tramite i badge vengano incrociati con altri dati al fine di ricostruire gli spostamenti e l'attività dei lavoratori all'interno dell'azienda. In tal senso il Garante[20] ha previsto che i dati raccolti attraverso i dispositivi di registrazione degli accessi e delle presenze devono essere alloggiati su un server diverso da quello in cui vengono inserite le informazioni sulle prestazioni lavorative.[21]

In riferimento al dettato del nuovo articolo 4, è importante stabilire cosa si intenda nello specifico per strumenti di registrazione degli accessi e delle presenze. Possono certamente considerarsi tali i tesserini che rilevano il passaggio da specifiche aree aziendali, non sono invece classificabili come tali ai fini dell'applicazione delle disposizioni di cui all'art. 4 co. 2 quei sistemi che consentono di monitorare costantemente gli spostamenti dei lavoratori all'interno dell'azienda.

In tal senso la tecnologia RFDI[22], acronimo di Radio Frequency Identification, che può essere utilizzata come alternativa a badge e tesserini magnetici, permette di monitorare dove si trovi il lavoratore in qualsiasi momento

---

[19] C. Zoli, E. Villa, *Gli strumenti di registrazione degli accessi e delle presenze*, in P. Tullini, (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, op. cit, pag. 127

[20] Autorità Garante per la protezione dei dati personali, prot. n. 17197 e 46087 del 2006.

[21] C. Zoli, E. Riva, ivi, pag. 128

[22] Si tratta di un sistema di identificazione automatica che utilizza onde radio per rilevare, identificare e tracciare, oggetti, animali e persone. Si basa su un sistema di comunicazione tra un lettore RFDI e un tag RFDI, un piccolo dispositivo elettronico che contiene un microchip e un'antenna.

durante l'orario di lavoro.

La pervasività di tale sistema di rilevazione lo rende particolarmente rischioso per la privacy e il Garante ne ha limitato l'utilizzo alle situazioni che lo rendano necessario per motivi di sicurezza, ad esempio per monitorare l'accesso a determinate aree aziendali che necessitano di particolari controlli; in tal caso deve essere formalizzato quanto previsto all'articolo 37 del Codice Privacy, ovvero la notifica al Garante, nonché deve essere fornita un'informativa specifica ai lavoratori interessati.[23]

## 1.7. L'utilizzo di dati biometrici

La biometria è definita come l'insieme delle tecniche di identificazione o di misurazione dell'essere umano attraverso la rilevazione di determinate caratteristiche fisiche o comportamentali che vengono tradotte in sequenze matematiche e conservate in banche dati elettroniche.[24]

L'utilizzo tradizionale dei dati biometrici è finalizzato a procedure di identificazione e di verifica dell'identità, che in campo lavoristico vedono come principale sviluppo applicativo la gestione degli accessi e la rilevazione delle presenze.

La biometria permette di cambiare l'oggetto dell'identificazione che passa da un accessorio che il lavoratore porta con sé, ovvero una chiave, un badge o una password, all'identificazione tramite una caratteristica fisica del soggetto, marginalizzando così l'eventuale errore di riconoscimento.

Le tecniche di rilevazione dei dati biometrici possono perciò rappresentare un

---

[23] C. Zoli, E. Riva, op. cit. pag. 132-134. Vedi anche Garante privacy, *"Etichette intelligenti" (Rfid): il Garante individua le garanzie per il loro uso - 9 marzo 2005*, doc. web 1109493, in www.garanteprivacy.it

[24] C. Sarra, *L'uso dei dati biometrici nelle procedure di reclutamento al lavoro mediante strumenti di Intelligenza Artificiale. Difficoltà normative multilivello*, in Journal of Ethics and Legal Technologies, Volume 4(2), novembre 2022, pag. 28

rischio per la privacy del lavoratore e pertanto il Garante si è pronunciato nel senso di limitare l'utilizzo di tale tecnologia a quelle occasioni nelle quali i motivi di sicurezza prevalgono sul diritto alla riservatezza.

Le caratteristiche dell'impronta digitale o della topografia della mano potranno essere utilizzate ad esempio per autorizzare l'accesso ad aree e locali ritenuti "sensibili", oppure per consentire l'utilizzo di apparati e macchinari pericolosi ai soli soggetti qualificati, ritenendo in tale ipotesi sufficiente l'informativa ai lavoratori e non necessario il consenso.[25]

Nel pubblico impiego si è in più occasioni valutato l'utilizzo di sistemi di rilevazione delle presenze tramite lettura dei dati biometrici per contrastare il diffuso fenomeno dell'assenteismo,[26] tanto che il Garante si è pronunciato in più occasioni in riferimento alle istanze presentate dalle pubbliche amministrazioni per richiedere l'autorizzazione all'utilizzo di tali particolari sistemi di monitoraggio.

Citiamo ad esempio il provvedimento n. 4430740 del 25 ottobre 2015 sulla rilevazione delle presenze dei dipendenti di un Comune tramite un sistema biometrico basato sul trattamento di impronte digitali. Il Garante in tale occasione si pronunciò contro la legittimità del provvedimento comunale in quanto carente nel motivare la necessità di ricorrere a tale strumento in alternativa ad altri strumenti automatizzati quali ad esempio i badge, normalmente utilizzati dalle pubbliche amministrazioni, evidenziando come il principio di necessità debba sempre essere il faro che illumina le scelte del datore di lavoro.

La biometria è una scienza in continuo sviluppo e numerose sono le sue

---

[25] Garante privacy, *Schema di provvedimento in tema di riconoscimento biometrico e firma grafometrica*, doc 3132642 e Garante privacy, *Provvedimento generale prescrittivo in tema di biometria*, 12 novembre 2014

[26] V. Maio, *Il regime delle autorizzazioni del potere di controllo del datore di lavoro*, in P. Tullini (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, op. cit., pag. 85

potenzialità anche in altre attività e con diverse finalità.

In particolare, nell'ambito del recruiting i dati biometrici possono ad esempio essere utilizzati, insieme a quantità di altri dati raccolti e analizzati con tecniche di data mining, per generare un profilo di lavoratore ideale attraverso il quale effettuare una preselezione dei candidati, riducendo i tempi e i costi della selezione.

La disponibilità di immagini e video degli aspiranti lavoratori può consentire un'analisi più approfondita delle caratteristiche dei vari candidati, facilitando ad esempio la valutazione delle capacità comunicative non solo tramite il linguaggio utilizzato, ma anche attraverso lo screening del linguaggio paraverbale e delle espressioni facciali per ricostruire un profilo psicologico attendibile.[27]

Per la compatibilità dell'utilizzo dei dati biometrici nelle procedure di selezione del personale con le norme a protezione dei dati dei lavoratori si rinvia al capitolo 3.

[27] C. Sarra, op. cit., pag. 35

# CAPITOLO 2

# IL QUADRO NORMATIVO DI RIFERIMENTO

## 2.1 I diritti fondamentali dei lavoratori nella Costituzione

La tutela dei diritti fondamentali in materia di lavoro è indubbiamente sancita dalla Costituzione, che all'articolo 1 riconosce al lavoro un valore fondante della Repubblica e all'articolo 4 riconosce ai cittadini il diritto al lavoro, quale mezzo atto a garantirne l'uguaglianza e permetterne lo sviluppo personale.

Nell'analisi delle norme che integrano il quadro dei principali diritti costituzionalmente tutelati, oltre all'articolo 2 (diritti inviolabili della persona), all'articolo 3 (uguaglianza formale e sostanziale), all'articolo 13 (diritti inviolabili della libertà personale), e all'articolo 15 (libertà di comunicazione e segretezza della corrispondenza) relativi a diritti fondamentali della persona, troviamo una serie di articoli espressamente dedicati alla salvaguardia dei diritti dei lavoratori.

Non troviamo nella Costituzione una norma rubricata diritto alla riservatezza; tuttavia, anche se non espressamente richiamato è un diritto riconosciuto attraverso le disposizioni che si riferiscono all'integrità e alla dignità della persona. A tal proposito rilevano l'art. 2 in materia di diritti inviolabili della persona e l'art. 15, che garantisce la libertà di comunicazione e la segretezza della corrispondenza e di ogni altra forma di comunicazione.[28]

In campo lavoristico assume particolare rilievo infine l'articolo 41, che sancisce la libertà di iniziativa economica privata ma stabilisce anche come questa "*non può svolgersi in contrasto con l'utilità sociale o in modo da recare danno alla salute, all'ambiente, alla sicurezza, alla libertà, alla dignità umana*".

[28] A. Ingrao, *Il controllo a distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata*, Cacucci Editore, Bari, 2018, pag. 17

## 2.2. Codice civile e rapporto di lavoro subordinato

Il Codice civile del 1942 ha voluto dare una regolamentazione sistematica alle norme in materia di lavoro nel libro V, che regola tutti gli aspetti dell'attività economica, tutelando il lavoro "*in tutte le sue forme organizzative ed esecutive, intellettuali, tecniche e manuali*".

Il codice considera il rapporto di lavoro subordinato quello socialmente più rilevante, modello normativo tipico e caratterizzato dallo scambio tra la retribuzione e una prestazione manuale o intellettuale.

Norma fondamentale è l'art. 2094, che definisce il lavoratore subordinato come colui che *"si obbliga mediante retribuzione a collaborare nell'impresa, prestando il proprio lavoro intellettuale o manuale alle dipendenze e sotto la direzione dell'imprenditore";* definendo il lavoratore subordinato, il codice individua le componenti essenziali del rapporto di lavoro.

Il lavoratore è il debitore della prestazione, colui che collabora nell'impresa svolgendo le proprie mansioni; l'imprenditore è il creditore, colui che dirige la prestazione e da cui il prestatore dipende, che sta a capo dell'impresa (art. 2086), dirige l'attività produttiva (art. 2082) e specifica le mansioni del lavoratore (artt. 2104 e 2103) direttamente o attraverso i sovraordinati del lavoratore stesso.

Il codice sancisce quindi l'attribuzione al datore di lavoro del potere direttivo sul lavoratore subordinato, conferendo al creditore della prestazione una posizione di supremazia contrattuale, funzionale alla realizzazione dell'interesse alla collaborazione del prestatore e alla direzione dell'attività lavorativa per il conseguimento del risultato utile atteso.[29]

Il contenuto del potere direttivo emerge dalla correlazione biunivoca con il contrapposto obbligo di diligenza del lavoratore subordinato disciplinato

[29] A. Ingrao, op. cit, pag. 13

all'art. 2104 c.c., che impone al prestatore di lavoro di usare la diligenza richiesta dalla natura della prestazione e dall'interesse dell'impresa e di "os*servare le disposizioni per l'esecuzione e per la disciplina del lavoro impartite dall'imprenditore e dai collaboratori di questo dai quali gerarchicamente dipende.*"

Il datore di lavoro è titolare di un potere di organizzazione e programmazione dell'operato della controparte, che viene esercitato in modo continuo e rafforzato per l'intera esecuzione del contratto. È proprio nell'attribuzione al creditore di un potere così pervasivo che si esplicita la particolarità della vicenda contrattuale lavoristica rispetto ad altri contratti di durata che hanno ad oggetto un *facere*, come l'appalto o il contratto d'opera.[30]

Il potere direttivo è accompagnato dal potere di controllo e dal potere disciplinare[31], peraltro quest'ultimo rappresenta un'anomalia rispetto alla logica paritaria dei rapporti contrattuali, dato che viene conferita ad un soggetto privato la possibilità di applicare sanzioni senza il filtro della magistratura.

Il datore di lavoro, quale creditore della prestazione, ha interesse all'adempimento da parte del lavoratore e avverte la necessità di valutare il comportamento della controparte per fargli mantenere un atteggiamento che si riveli quanto più conforme alla soddisfazione del suo interesse.

A tal fine rileva il potere di controllo, che non ha una specifica norma definitoria ma discende da quello direttivo e costituisce il collegamento tra il potere direttivo e il potere disciplinare, condividendo con essi da un lato la necessità di verificare le modalità di esecuzione della prestazione e dall'altro l'esigenza di ristabilire il corretto svolgimento dell'attività lavorativa in caso di inadempimento, al fine di garantire la continuità dell'attività d'impresa.

---

[30] A. Ingrao, op. cit., pag. 12

[31] Articolo 2106 cc: "L'inosservanza delle disposizioni … può dar luogo all'applicazione di sanzioni disciplinari, secondo la gravità dell'infrazione".

## 2.3. Lo Statuto dei lavoratori

La legge n. 300 del 1970 denominata Statuto dei lavoratori costituisce la piattaforma dei diritti fondamentali, civili e sociali dei lavoratori.

Tutto il Titolo I, in attuazione dell'articolo 41 della Costituzione, intende circoscrivere il potere datoriale per evitare che la condizione di subordinazione si trasformi in un rapporto di soggezione personale del lavoratore al datore di lavoro e, più in particolare, con l'art. 8 mira a tutelare la vita privata del lavoratore, imponendo una valutazione del lavoratore basata solo su criteri rigorosamente e specificatamente professionali.[32]

Per circoscrivere il divieto di indagine contenuto nell'art. 8 è evidentemente centrale il concetto di rilevanza ai fini dello svolgimento della prestazione delle informazioni acquisite, che l'articolo 8 definisce indagini.

L'articolo 8 va letto congiuntamente ad altre disposizioni dello Statuto. *In primis* l'articolo 1, che sancisce la libertà di opinione nei luoghi di lavoro, in considerazione del fatto che un'attività di schedatura provoca un'indiretta pressione suscettibile di limitare di fatto la libertà di manifestazione del pensiero[33]; d'altro lato l'art. 8, nella misura in cui preclude la raccolta di materiale informativo da porre a base di eventuali future discriminazioni, anticipa gli effetti della tutela antidiscriminatoria fornita dall'art. 15 e dalla legislazione successiva.

---

[32] L'art. 8 prevede che "è fatto divieto al datore di lavoro, ai fini dell'assunzione come nel corso di svolgimento del rapporto di lavoro, di 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":

[33] Nel 1971, anno successivo alla pubblicazione dello Statuto, vennero alla luce e furono oggetto di un caso giudiziario le schedature Fiat, un archivio aziendale contenente 354.077 schede personali, con informazioni su opinioni politiche e religiose, attività sindacale, condotta sessuale, abitudini dei dipendenti e dei candidati all'assunzione e dei loro familiari. Il clima del periodo fa supporre che il caso Fiat non rappresentasse però un unicum nel sistema imprenditoriale dell'epoca e che le pratiche datoriali di indagine su abitudini e opinioni dei lavoratori fossero abbastanza diffuse.

L'articolo 8 ha quindi un vasto campo di applicazione e ne consente l'adattabilità agli attuali scenari tecnologici. Infatti, il divieto riguarda sia la fase preassuntiva, sia quella di svolgimento del rapporto e le indagini vietate sono sia quelle svolte direttamente dal datore di lavoro e dai suoi collaboratori quanto quelle effettuate da terzi.[34]

Lo Statuto si occupa poi di disciplinare il potere di controllo, riservando una serie di articoli alla disciplina dei controlli uomo su uomo e l'articolo 4 dei controlli automatizzati.

Proprio questo articolo è il più rilevante dal punto di vista della tutela della riservatezza e dignità dei lavoratori, poiché l'utilizzo della tecnologia permette controlli sempre più occulti e pervasivi.

Il legislatore del 1970 aveva previsto regole imperative e rigorose: nel testo originale l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dei lavoratori era espressamente vietato.

Il secondo comma introduceva la possibilità di utilizzare tali strumenti solo per *esigenze organizzative e produttive ovvero dalla sicurezza del lavoro,* ma per la loro installazione rendeva obbligatorio il *previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna,* oppure, in mancanza di accordo, con provvedimento dell'Ispettorato del lavoro in esito alla presentazione di apposita istanza.

La norma, tuttavia, ha presentato negli anni notevoli difficoltà di interpretazione e applicazione, in particolare con riferimento ai controlli difensivi, ovvero i controlli messi in atto dal datore di lavoro per proteggere il patrimonio aziendale.

La giurisprudenza ha distinto in tal senso tra i controlli preterintenzionali,

[34] M. Aimo, *Dalle schedature dei lavoratori alla profilazione tramite algoritmi: serve ancora l'art. 8 dello Statuto dei lavoratori?*, Lavoro e diritto, anno XXXV, n. 3-7, estate-autunno 2021, Ed. Il Mulino, pag. 588

legittimi solo in caso di previo esperimento della procedura autorizzativa, e i controlli cosiddetti difensivi posti in essere dal datore di lavoro per la tutela del patrimonio aziendale contro eventuali illeciti del lavoratore.[35]

Per questi ultimi la giurisprudenza è intervenuta creando una forma di controllo non disciplinata dal vecchio articolo 4, rendendo di fatto possibili e regolamentando tali tipi di controllo attraverso l'individuazione di tre parametri, ovvero la presenza di un fondato sospetto della commissione di un illecito da parte del dipendente, la possibilità di utilizzare solo le informazioni raccolte dopo l'insorgere del sospetto e non quelle ricavabili ex ante dai controlli preterintenzionali e infine la necessità di limitare la raccolta delle informazioni a quelle proporzionate all'obiettivo.

L'inadeguatezza della norma rispetto a tali problematiche, nonché rispetto ai tempi (anche se la terminologia generica utilizzata dal legislatore ha permesso nei decenni successivi di poter estendere senza particolari difficoltà le previsioni normative anche alle nuove strumentazioni introdotte dal progresso tecnologico) ha portato alla necessità di revisione dello Statuto, evocata dalla Legge delega del Jobs Act n. 183/2014 e dall'articolo 23 del Decreto legislativo n.151/2015.[36]

L'attuale dettato dell'articolo 4 non prevede più il divieto assoluto di utilizzo di impianti audiovisivi e altri strumenti idonei al controllo a distanza come previsto dal comma 1 del vecchio testo e aggiunge un'ulteriore finalità che ne consente l'utilizzo, ora possibile *per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale. Resta la prescrizione del previo accordo sindacale o, in mancanza di accordo, previa autorizzazione della sede competente dell'Ispettorato nazionale del lavoro.*

---

[35] G. Busia, *Così vicini così distanti: i controlli da remoto del datore di lavoro e la riservatezza del dipendente*, Lavoro Diritti Europa, 2023/3, pag. 7

[36] P. Tullini, *La digitalizzazione del lavoro, la produzione intelligente e il controllo tecnologico dell'impresa*, in P. Tullini (a cura di), *Web e lavoro. Profili evolutivi di tutela*, op. cit., pag. 12

Alle esigenze organizzative e produttive e a quelle legate alla sicurezza è stata aggiunta la tutela del patrimonio, in recepimento dell'esigenza precedentemente evidenziata e risolta dalla giurisprudenza.

Se non è più previsto un esplicito divieto di utilizzo di strumenti con finalità esclusiva di controllo a distanza, dalla struttura lessicale e dalla lettura delle indicazioni contenute nella Legge delega tale divieto risulta tuttavia implicitamente conservato.[37]

La prima grande novità introdotta dalla riforma è prevista al comma 2, che esclude dalla procedura autorizzativa del comma 1 gli *strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.*

Tale disposizione ben si sposa con le innovazioni tecnologiche, che hanno completamente modificato le modalità di resa della prestazione e di fatto reso indispensabili una serie di strumenti che possono per loro natura essere utilizzati anche per effettuare il controllo.

Il comma 3 infine estende la possibilità di utilizzo delle informazioni raccolte per tutti i fini connessi al rapporto di lavoro, purché il trattamento sia preceduto da un'adeguata informazione sulle finalità e modalità di raccolta e sia rispettato il Codice privacy, anche in questo caso allargando le maglie del potere datoriale.

Restano confermate invece le sanzioni disciplinari in caso di violazione degli obblighi.

## 2.4 Il Codice privacy

La direttiva n. 95/46/CE del Parlamento Europeo e del Consiglio fu attuata in

[37] A. Sitzia, *Personal computer e controlli tecnologici del datore di lavoro nella giurisprudenza*, ADL 3/2017, Wolters Kluwer Italia s.r.l., pag. 826

Italia dapprima con la Legge 31 dicembre 1996 n. 675 e in seguito con il D. Lgs. 30 giugno 2003 n. 196, denominato Codice Privacy, che rappresenta la prima razionalizzazione sistematica sulla protezione dei dati personali nel trattamento automatizzato.[38]

L'articolo 1 sanciva espressamente il diritto alla protezione dei dati personali all'interno dei diritti della persona già previsti dagli articoli da 5 a 10 del Codice civile e l'articolo 2 lo annovera accanto al diritto alla dignità, alla libertà personale e alla riservatezza.

L'impianto normativo prevedeva la libera circolazione dei dati come regola; la tutela principale era garantita attraverso la definizione delle regole per le operazioni di raccolta, gestione, conservazione e utilizzo delle informazioni personali che il titolare del trattamento era tenuto ad osservare.

La norma stabiliva un diverso livello di rischio attraverso la distinzione tra dati comuni, per il trattamento dei quali era sufficiente il consenso informato dell'interessato, e dati sensibili, idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, lo stato di salute e la vita sessuale, che potevano diventare fonte di discriminazione e che quindi necessitavano di misure di sicurezza rafforzate con una specifica procedura di autorizzazione da parte del Garante per la protezione dei dati personali.[39]

---

[38] A. Ingrao, op. cit, pagg. 60-63

[39] Articolo 37: Il titolare notifica al Garante il trattamento di dati personali cui intende procedere, solo se il trattamento riguarda:
a) dati genetici, biometrici o dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica;
b) dati idonei a rivelare lo stato di salute e la vita sessuale, trattati a fini di procreazione assistita, prestazione di servizi sanitari per via telematica relativi a banche di dati o alla fornitura di beni, indagini epidemiologiche, rilevazione di malattie mentali, infettive e diffusive, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria;

Un sistema preventivo di controlli, disciplinato agli articoli 17 e 37, era previsto anche per quei trattamenti che potevano presentare un rischio elevato a causa delle tecnologie impiegate o della particolare natura dei dati trattati.
Alcune specifici limiti alla libertà di circolazione erano poi individuati in alcuni casi specifici, in particolare per quanto riguarda i diritti dei lavoratori gli articoli 113 e 114 richiamavano espressamente quanto previsto agli articoli 8 e 4 dello Statuto dei lavoratori.
Il codice prevedeva anche una serie di diritti per l'interessato, che poteva esercitare il controllo sulle proprie informazioni e che gli consentivano la facoltà di ottenere l'accesso, l'aggiornamento, la rettifica, l'integrazione, la trasformazione e la cancellazione dei dati.
L'elemento più significativo era la fissazione di alcune regole di principio, volte a limitare l'attività di raccolta dei dati personali e le modalità di trattamento.
L'articolo 11 obbligava al rispetto dei principi di correttezza, di necessità e di finalità della raccolta; l'utilizzo dei dati raccolti in violazione di tali principi li rendeva inutilizzabili, impedendo quindi l'ammissibilità in giudizio del materiale probatorio raccolto dal datore di lavoro in violazione dell'articolo 4 delle Statuto, come integrato dalle norme del Codice Privacy.

---

c) dati idonei a rivelare la vita sessuale o la sfera psichica trattati da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale;
d) dati trattati con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti;
e) dati sensibili registrati in banche di dati a fini di selezione del personale per conto terzi, nonché dati sensibili utilizzati per sondaggi di opinione, ricerche di mercato e altre ricerche campionarie;
f) dati registrati in apposite banche di dati gestite con strumenti elettronici e relative al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti.

L'integrazione e l'armonizzazione di tali norme ha faticato ad affermarsi; un ruolo fondamentale è stato svolto dal Garante per la protezione dei dati personali, che ha emanato una serie di linee giuda e provvedimenti contenenti indicazioni in materia di trasparenza, prevenzione e proporzionalità e che specificavano le intersezioni con le norme statutarie.

Le indicazioni contenute nelle linee guida si traducevano nel divieto di controlli occulti, l'obbligo di fornire l'informativa, il divieto di controlli prolungati, continui e indiscriminati, l'obbligo di preferire misure di tipo organizzativo, volte a prevenire ex ante la commissione di illeciti, piuttosto che controlli mirati sulla verifica del comportamento dei dipendenti.Tuttavia tali indicazioni, trattandosi appunto di linee giuda, sono spesso rimaste inosservate da parte degli operatori dei vari settori e hanno generato a livello giurisprudenziale l'abbondante casistica in materia di "controlli difensivi".

Tale inosservanza è altresì riferibile alla mancanza, nella parte sanzionatoria del Codice Privacy, di regole dirette a obbligare i datori di lavoro a conformare la propria organizzazione al rispetto dei principi di necessità, proporzionalità e finalità.

Il nuovo quadro regolativo definito in seguito all'applicazione del Regolamento Ue 979/2016 mira a porre rimedio a tali difficoltà.

In seguito all'entrata in vigore del GDPR, il Codice Privacy è stato modificato con l'entrata in vigore del Decreto Legislativo 10 agosto 2018 n. 101, che ha determinato la cancellazione delle norme incompatibili e l'adeguamento delle norme in materia di trasparenza al nuovo dettato sovranazionale.

## 2.5 Le fonti europee in materia di diritto alla riservatezza

### 2.5.1. La tutela nei trattati dell'Unione

La Convenzione Europea dei Diritti dell'Uomo (Cedu) all'articolo 8 in materia

di "Diritto al rispetto della vita privata e familiare" dispone che *"ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza"*; al secondo paragrafo sono enucleati i presupposti che legittimano lo Stato membro a sottoporre a restrizione l'esercizio di tale diritto: *"non può esservi ingerenza di un'autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del Paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui"*.

Il diritto alla riservatezza è espressamente previsto anche all'articolo 7 della Carta di Nizza (Carta dei diritti fondamentali dell'UE), che prevede che "*ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni*", mentre l'articolo 8 è dedicato alla "protezione dei dati di carattere personale" e stabilisce che "*ogni individuo ha diritto alla protezione dei dati e di carattere personale che lo riguardano*" e che "*tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge*."

Tali norme obbligano gli Stati membri a conformarsi e rispettare tali principi e a procedere alla definizione e individuazione dei diritti oggetto di bilanciamento: nel nostro ordinamento il diritto alla riservatezza, che un diritto inviolabile ma relativo, è posto in bilanciamento con la libertà d'impresa.

Per l'interpretazione dell'articolo 8 della Cedu in riferimento al potere di controllo assume rilevanza fondamentale la giurisprudenza della Corte Europea per i Diritti Umani, in particolare alcune sentenze in materia di controlli tecnologici occulti, tra le quali hanno assunto importanza

significativa quelle relative ai casi Barbulescu e Lopez Ribalda.

La pronuncia della Grande Camera della Corte di Strasburgo sul caso Barbulescu[40] è riferita alla vicenda di un lavoratore rumeno, licenziato dal proprio datore di lavoro perché a seguito dei controlli operati sul corretto utilizzo dell'account Yahoo Messanger del dipendente (creato su indicazione del datore di lavoro per interagire in modo più efficace con i clienti) era emerso un utilizzo di tale strumento durante l'orario di lavoro per inviare messaggi privati alla famiglia e alla fidanzata. Tali messaggi contenevano informazioni sulla vita privata, lo stato di salute e la vita sessuale del dipendente; tuttavia, il regolamento interno aziendale prevedeva il divieto di utilizzare gli strumenti aziendali per motivi privati.

Il lavoratore, che si era rivolto senza successo alle corti nazionali per ottenere il riconoscimento dell'illegittimità del provvedimento disciplinare e del conseguente licenziamento, si era quindi rivolto alla Corte europea per i diritti dell'uomo, lamentando il mancato rispetto dell'art. 8 della Cedu.

I giudici europei hanno in prima istanza considerato ragionevole il controllo posto in essere dal datore di lavoro, valutando che avesse operato un corretto bilanciamento tra i suoi interessi e il diritto alla privacy del dipendente.[41]

Il lavoratore si è quindi rivolto alla Gran Camera, che con la sentenza del 5 settembre 2017 ha ribaltato la precedente decisione affermando l'esistenza della violazione dell'art. 8.

La Corte ha ritenuto che vi fosse lesione del bene giuridico della "vita privata" e che tale bene debba essere espressamente tutelato anche nell'ambito del

[40] Corte Europea dei diritti dell'uomo 5 settembre 2017, ricorso n. 61496/08, Causa Barbulescu c. Romania, in https://www.giustizia.it/giustizia/it/mg_1_20_1.page?contentId=SDU118786

[41] Ambrosino A, Riflessioni sul potere datoriale di controllo alla luce delle pronunce della Corte europea dei diritti dell'uomo sul caso Barbulescu c. Romania, Variazioni su temi di Diritto del lavoro, Giappichelli editore, Fascicolo 1/2018, pag. 260

rapporto di lavoro.[42]

La sentenza cita una serie di precedenti in materia di violazione della privacy del dipendente attraverso l'utilizzo dei controlli tecnologici e, in particolare, fornisce una serie di indicazioni per vagliare l'ammissibilità del controllo.

Il giudice dovrebbe verificare se il dipendente sia stato preventivamente informato riguardo alla possibilità del controllo e della sua attuazione, quanto sia esteso il controllo e il grado di intrusione nella privacy del lavoratore, se il datore abbia fornito giustificazioni legittime del controllo delle comunicazioni e del loro contenuto, se fosse stato possibile porre in essere un controllo meno invasivo, quali siano le conseguenze del monitoraggio per il lavoratore e quale l'uso fatto dal datore di lavoro dei risultati ottenuti, se siano state predisposte adeguate misure di salvaguardia nei confronti del lavoratore.

Secondo la corte Edu bisogna, inoltre, che le autorità nazionali assicurino al dipendente, la cui comunicazione sia stata monitorata, di poter disporre di un rimedio innanzi all'organo giudiziario competente ad accertare se i criteri predetti siano stati osservati e se le misure contestate siano legittime.[43]

Altra sentenza fondamentale è quella relativa al caso Lopez Ribalda and others v. Spain[44], che riguarda la vicenda di alcuni dipendenti di un supermercato, licenziati in seguito ad alcuni furti commessi dagli stessi. In questo caso alla prima sentenza favorevole ai lavoratori è seguita la seconda pronuncia a favore del datore di lavoro, per la quale la Grande Camera ha utilizzato i principi e le regole per verificare la liceità del controllo enunciati nel caso Barbulescu, anche se non ha ritenuto a tal fine necessaria la previa

---

[42] Vedi ad esempio la sentenza Copland v. United Kindom del 3 aprile 2007 relativa all'attività di monitoraggio del datore sulle telefonate, le mail e l'uso di internet da parte della dipendente

[43] M. Tufo, *Potere di controllo datoriale vs privacy del lavoratore: alla ricerca delle coordinate di ammissibilità dei controlli occulti*, Studium Iuris 7-8/2020, Wolters Kluwer Italia srl, pag. 854

[44] Corte Europea dei diritti dell'uomo, 17 ottobre 2019, caso Lopez Ribalda altri c. Spagna (n. 2), ricorsi n. 1874/13 e 8567/13, con traduzione a cura di F. Perrone in https://www.lavorodirittieuropa.it/images/lopez_ribalda_italiano.pdf

informazione ai lavoratori.[45]

Il "decalogo" stilato dal giudice del caso Barbulescu, quindi, non viene interpretato come tassativo, ma come una sintesi di indici particolarmente significativi che il giudice dovrà applicare al caso concreto per definire se il controllo è proporzionato al fine che lo giustifica.[46]

### 2.5.2. La Raccomandazione CM/Rec(2015)5 del Comitato dei Ministri agli stati membri sul trattamento di dati personali nel contesto occupazionale.

Il 1° aprile 2015 il Consiglio d'Europa ha adottato la Raccomandazione n. 5 in materia di trattamento dei dati personali nell'ambito del rapporto di lavoro, andando a sostituire la precedente Raccomandazione n. 2 del 1989.

Nella prima parte della Raccomandazione si richiamano i principi generali in materia di protezione dei dati personali, già contenuti nella direttiva madre e successivamente ribaditi dal Regolamento UE n. 2016/679.[47]

Tale atto prevede che i datori di lavoro debbano minimizzare il trattamento dei dati allo stretto necessario per il perseguimento dello scopo del caso concreto e debbano adottare le misure appropriate ad assicurare il rispetto della riservatezza dei lavoratori. (art. 4).

I dati dovrebbero essere raccolti, se possibile, direttamente presso l'interessato e, qualora fosse necessario raccogliere informazioni presso terzi (ad esempio

---

[45] Così la sentenza al punto 134: "Nel caso di specie, avuto riguardo in particolare al grado di intrusione concretamente effettuato nella privacy dei ricorrenti […] e allo scopo legittimo che ha giustificato l'installazione degli strumenti di videosorveglianza, la Corte ritiene che le corti nazionali non hanno oltrepassato il margine di apprezzamento che compete alle autorità nazionali nella valutazione della proporzionalità della misura adottata rispetto al fine concretamente perseguito."

[46] Tufo, op. cit, pag. 855

47 A. Sitzia, *I controlli a distanza dopo il Jobs Act e la Raccomandazione R (2015)5 del Consiglio d'Europa*, Il Lavoro nella giurisprudenza, 7/2015, Wolters Kluwer Italia s.r.l., pag. 677

le referenze di un precedente datore di lavoro), il lavoratore dovrebbe essere informato preventivamente.

Si richiamano inoltre i principi della pertinenza e della non eccedenza dei dati rispetto alle necessità del datore di lavoro e alla necessità che il loro trattamento sia limitato agli scopi di lavoro dichiarati.

L'articolo 10 introduce il principio di trasparenza del trattamento in base al quale il datore di lavoro deve fornire al lavoratore un'informativa chiara e completa in merito ai dati trattati, allo scopo del trattamento, ai destinatari della divulgazione, ai mezzi per esercitare l'accesso, la rettifica e l'obiezione al trattamento dei dati.

Rilievo particolare è dato infine alla sicurezza e conservazione dei dati (art. 12-13).

Nella seconda parte della Raccomandazione si individuano con maggiore precisione alcune particolari tipologie di trattamento, in particolare le possibili forme di controllo derivanti dall'utilizzo delle nuove tecnologie: Internet e comunicazioni elettroniche sul luogo di lavoro (art. 14), Sistemi informativi e tecnologie per la sorveglianza dei dipendenti, compresa la videosorveglianza (art. 15), apparecchiature in grado di rivelare l'ubicazione dei dipendenti (art. 16), meccanismi interni di segnalazione (art. 17), dati biometrici (art. 18), test psicologici, analisi ed analoghe procedure (art. 19) e altri specifici trattamenti che rappresentino specifici rischi per i diritti, ponendo nuove garanzie a tutela dei lavoratori, soprattutto in materia di trasparenza.

La Raccomandazione sottolinea che il datore di lavoro dovrebbe astenersi da "*ingerenze ingiustificabili e irragionevoli nella vita privata del dipendente*", tuttavia non preclude la possibilità di permettere al datore di lavoro di accedere ai dati raccolti tramite le succitate tecnologie. Tale accesso deve però essere necessario per motivi di sicurezza o per tutelare altri legittimi interessi, ma dovrà essere

il meno intrusivo possibile e solo previa informazione del dipendente interessato.

### 2.5.3. Il Regolamento Europeo per la protezione dei dati

Il 27 aprile 2016 ha visto la luce il Regolamento (UE) n. 2016/679 del Parlamento Europeo e del Consiglio, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libertà di circolazione di tali dati. Il Regolamento è divenuto esecutivo nel nostro Paese il 18 maggio 2018, comportando la definitiva abrogazione della direttiva precedente e di alcune parti del Codice privacy.

La novità riguarda innanzitutto il tipo di provvedimento utilizzato, infatti nella disciplina di tale materia il legislatore europeo sceglie di sostituire una direttiva con un regolamento, la cui efficacia vincolante è immediata[48]: Tale scelta esprime la convinzione del legislatore europeo che non sia sufficiente armonizzare la legislazione dei vari Stati in materia di protezione dei dati personali, ma che l'evoluzione tecnologica richieda regole uniformi applicabili in tutti gli Stati dell'Unione.[49]

Dal punto di vista territoriale, il Regolamento troverà applicazione se il soggetto a cui si riferiscono i dati si trovi realmente o virtualmente nel territorio europeo oppure se il titolare o il responsabile del trattamento è stabilito nell'Unione, anche se il trattamento è effettuato all'esterno dell'Unione stessa.[50]

Il Regolamento si occupa di disciplinare il trattamento dei dati personali[51],

---

[48] In questo caso il Regolamento, per sua espressa previsione, sostituirà la disciplina contenuta nella Direttiva previgente solo nel 2018, dando così agli Stati membri due anni di tempo per adeguarsi alle nuove previsioni; in Italia il Regolamento è quindi applicato dal 25 maggio 2018.

[49] A. Ingrao, op. cit, pag. 77

[50] C. Ogriseg, *Il Regolamento UE n. 2016/679 e la protezione dei dati personali nelle dinamiche giuslavoristiche: la tutela riservata al dipendente*, in LLI, vol. 2. n. 2, 2016, pag. 37-38

[51] All'articolo 4 il Regolamento definisce il dato personale come "qualsiasi informazione

nonché la loro circolazione nel rispetto del diritto alla protezione dei dati, considerato come diritto e fondamentale.

I considerando sottolineano la necessità di garantire i diritti fondamentali, "*in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica*".

Il legislatore europeo evidenzia anche come la rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali, "*in quanto è aumentata in modo significativo la portata della condivisione e della raccolta di dati personali e la tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività*".

La necessità di garantire un quadro più solido e coerente in materia di protezione dei dati nell'Unione è ritenuta fondamentale per creare il clima di fiducia che consentirà lo sviluppo dell'economia digitale in tutto il mercato interno.

Particolare rilevanza è data anche all'opportunità che le persone fisiche, che sempre più spesso rendono disponibili al pubblico su scala mondiale le loro informazioni personali, abbiano il controllo dei dati personali che li riguardano.

Il Regolamento introduce, rispetto alla normativa precedente, un diverso approccio alla materia, sostituendo una disciplina di carattere autorizzatorio

---

concernente una persona fisica identificata o identificabile, l'interessato"; si considera identificabile la persona che può essere identificata, direttamente o indirettamente, con particolare riferimento "*a un identificativo come il nome, un numero di identificazione, i dati relativi all'ubicazione, un identificativo on line o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*."

con una regolamentazione basata sul principio di responsabilizzazione del titolare del trattamento, che dovrà essere in grado di dimostrare l'adozione e l'efficace implementazione di un modello organizzativo che garantisca il rispetto delle norme contenute nel Regolamento e il contenimento dei rischi per la dignità, riservatezza, libertà e autodeterminazione degli interessati.[52]

Il rischio può derivare dall'esecuzione di un trattamento non conforme ai principi dettati dalla disciplina in materia di dati personali, oppure in violazione delle regole per la sicurezza del trattamento dei dati, che può causare la distruzione, la perdita, la modifica, la diffusione non autorizzata o l'accesso ai dati trattati.

Il Regolamento, accanto alle norme generali sulla protezione dei dati personali dei lavoratori riserva a ciascuno Stato membro la facoltà di prevedere, tramite leggi e contratti collettivi, discipline più specifiche rispetto a quelle generali contenute nel Regolamento.[53]

Le normative speciali attuate dai singoli Stati dovranno altresì tener conto di quanto previsto dalla succitata Raccomandazione CM/Rec(2015)5.

Con riferimento ai dati dei lavoratori, la protezione riguarda tutte le

---

[52] A. Ingrao, op. cit., pag. 126

[53] Così recita l'articolo n. 88: "*Gli Stati membri possono prevedere, con legge o tramite contratti collettivi, norme più specifiche per assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro, in particolare per finalità di assunzione, esecuzione del contratto di lavoro, compreso l'adempimento degli obblighi stabiliti dalla legge o da contratti collettivi, di gestione, pianificazione e organizzazione del lavoro, parità e diversità sul posto di lavoro, salute e sicurezza sul lavoro, protezione della proprietà del datore di lavoro o del cliente e ai fini dell'esercizio e del godimento, individuale o collettivo, dei diritti e dei vantaggi connessi al lavoro, nonché per finalità di cessazione del rapporto di lavoro.* E il considerando 155*: Il diritto degli Stati membri o i contratti collettivi, ivi compresi gli «accordi aziendali», possono prevedere norme specifiche per il trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro, in particolare per quanto riguarda le condizioni alle quali i dati personali nei rapporti di lavoro possono essere trattati sulla base del consenso del dipendente, per finalità di assunzione, esecuzione del contratto di lavoro, compreso l'adempimento degli obblighi stabiliti dalla legge o da contratti collettivi, di gestione, pianificazione e organizzazione del lavoro, parità e diversità sul posto di lavoro, salute e sicurezza sul lavoro, e ai fini dell'esercizio e del godimento, individuale o collettivo, dei diritti e dei vantaggi connessi al lavoro, nonché per finalità di cessazione del rapporto di lavoro.*

informazioni raccolte in occasione dell'assunzione e della gestione del rapporto di lavoro, ma anche le informazioni rilasciate durante la navigazione sui siti web tramite strumenti elettronici forniti dall'azienda, le informazioni connesse all'uso delle mail nonché le informazioni salvate in profili personali dei social network e riferibili al dipendente.[54]

La definizione di dato personale contenuta all'articolo 4 del regolamento evidenzia infatti come essa ricomprenda qualsiasi dato e/o informazione attinente a un lavoratore identificato o identificabile, specificando come la persona possa essere indirettamente identificata, direttamente o indirettamente, non solo tramite il nome o un numero di identificazione, ma anche attraverso *"un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale."*

Il Regolamento ripropone la distinzione già contenuta nel Codice Privacy tra dati comuni e dati sensibili, definiti come categorie particolari di dati; l'articolo 9 non vieta l'utilizzo delle informazioni sensibili del lavoratore, ma ne consente il trattamento qualora necessario, obbligando il datore di lavoro ad una valutazione del rischio rispetto alle finalità del trattamento.[55]

Particolari divieti sono previsti qualora si trattino i dati in modo automatizzato, in particolare l'articolo 22 prescrive che "l'*interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona".*

A tale divieto sono previste alcune eccezioni, in particolare la necessità di concludere o eseguire un contratto, la presenza di norme autorizzative a livello europeo o nazionale, il consenso dell'interessato. In ambito lavorativo,

[54] C. Ogriseg, op. cit., pag. 36
[55] A. Ingrao, op. cit, pag. 89

tuttavia, il consenso può sempre essere potenzialmente viziato o non valido per la posizione debole che il lavoratore ricopre nei confronti del datore di lavoro.

All'articolo 4 la profilazione è definita come qualsiasi forma di trattamento automatizzato di dati personali consistente nel loro utilizzo per valutare determinati aspetti relativi a una persona fisica, in particolare per "*analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica*".

L'impiego di tecnologie in grado di sostituirsi all'uomo nell'attività di conoscenza e valutazione di un soggetto al fine di raggiungere un determinato scopo individua nuovi rischi per i diritti della personalità e quindi si è resa necessaria una specifica norma a salvaguardia di tali diritti.

Il Regolamento non vieta la profilazione, anzi prevede che il divieto possa essere rimosso qualora sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento, sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento oppure si basi sul consenso esplicito dell'interessato;[56] l'interessato dovrà tuttavia essere preventivamente ed adeguatamente informato e potrà chiedere l'umanizzazione del giudizio finale, esercitando il diritto di richiedere l'intervento umano al titolare del trattamento, di esprimere la propria opinione e di contestare la decisione, riequilibrando così la sproporzione tra le parti del contratto.

Importante novità è l'inserimento tra i dati particolari dei dati genetici e biometrici, nonché particolari garanzie per i dati giudiziari, relativi a condanne penali e reati.

[56] A. Ingrao, op. cit, pag. 86-87

L'articolo 5 del Regolamento identifica i principi che regolano il trattamento dei dati, dalla fase di acquisizione fino a quella successiva di conservazione.
I principi di legittimità, correttezza, trasparenza, limitazione delle finalità, minimizzazione e responsabilizzazione obbligano il titolare a conformare la propria azione nell'esercizio del controllo a distanza dei lavoratori.
Per il principio di legittimità risultano utilizzabili solo quei dati che siano stati raccolti e conservati con modalità conformi alla legge. Non sono quindi ad esempio utilizzabili i dati raccolti in violazione degli articoli 8 e 4 dello Statuto dei lavoratori.
L'obbligo di trasparenza e di limitazione delle finalità pongono un limite ai datori di lavoro, che possono trattare i dati soltanto per finalità "*determinate, esplicite e legittime*": deve quindi esserci uno scopo ben definito, che deve essere esplicitato nell'informativa e rispettato per l'intera durata del trattamento; eventuali finalità ulteriori devono essere compatibili con quelle inizialmente dichiarate.
Altro principio fondamentale è quello di minimizzazione dei dati, che prevede che essi siano "*adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati*"; questo presuppone anche che il trattamento dei dati personali e identificativi sia limitato dal datore di lavoro ai casi in cui è strettamente necessario, preferendo ogniqualvolta sia possibile l'utilizzo di dati anonimi o aggregati o l'utilizzo di altri mezzi meno invasivi per raggiungere le proprie legittime finalità.
Il principio di responsabilizzazione prevede infatti che il datore di lavoro, per il rispetto dei suddetti principi, ponga in essere tutte le misure organizzative necessarie a prevenire eventuali trattamenti illeciti, con l'adozione di politiche adeguate in materia di controllo.
Infine, i principi di esattezza, limitazione della conservazione, integrità e

riservatezza hanno lo scopo di garantire il mantenimento di determinati requisiti dei dati durante la loro conservazione.

Il Regolamento all'articolo 25 declina in tal senso i cosiddetti principi di privacy by design e privacy by default.[57]

Il primo garantisce la protezione dei dati a partire dalla fase di ideazione e progettazione, assicurando la prevenzione degli abusi attraverso idonee misure tecniche e organizzative. Si prevede infatti che sia il titolare del trattamento a "*mettere in atto misure tecniche e organizzative adeguate, quali la pseudonomizzazione*[58]*, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati."*[59]

La privacy by default prevede che il titolare del trattamento dei dati "*metta in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento"* e che i dati personali non siano accessibili, per impostazione predefinita, a un numero di persone indefinito senza che vi sia l'intervento umano.

Il titolare deve essere in grado di dimostrare l'attuazione di tali prescrizioni, nonché egli è tenuto a verificare ex post e a modificare ed aggiornare le misure adottate ogniqualvolta si renda necessario (vedi articolo 24).

L'impostazione del Regolamento, con un nuovo approccio sistemico che

---

[57] A. Ingrao. op. cit, pag. 130-133

[58] La pseudonimizzazione comporta il trattamento dei dati personali in modo tale che gli stessi dati non possano più essere attribuiti a una persona specifica senza l'utilizzo di informazioni aggiuntive, perché i dati direttamente identificativi, come ad es. cognome e nome, sono sostituiti con dati indirettamente sostitutivi come ea es. un numero di classificazione.

[59] C. Del Federico, *Il trattamento dei dati personali dei lavoratori e il Regolamento 2016/679/UE. Implicazioni e prospettive*, in Tullini P. (a cura di), *Web e lavoro. Profili evolutivi e di tutela*, op.cit., pag. 73

promuove analisi e valutazioni preventive per individuare i possibili rischi per la sicurezza dei dati[60], prevede anche che l'interessato non abbia un ruolo esclusivamente passivo, ma che gli siano riconosciuti una serie di diritti. In primo luogo, il diritto di accesso ai propri dati (articolo 15) e la possibilità di poter intervenire sul loro trattamento attraverso la rettificazione e l'integrazione, la cancellazione dei dati, la limitazione del trattamento e la portabilità del dato (sezione 3 del Regolamento, articoli 16-20).[61]

Come poco sopra ricordato, il Regolamento prevede poi agli articoli 21 e 22 la possibilità per l'interessato di opporsi a trattamenti quali la profilazione, ottenendo di non essere sottoposto a decisioni basate su trattamenti esclusivamente automatizzati[62].

Per l'esercizio di tali diritti ricopre un ruolo fondamentale l'obbligo previsto per i titolari di fornire agli interessati un'adeguata e specifica informazione rispetto ai dati trattati, sia quando sono forniti direttamente dall'interessato (articolo 13), sia quando non siano raccolti presso di esso (articolo 14).

Il Regolamento introduce una nuova figura, il DPO (Data Protection Officer), il responsabile della protezione dei dati che in azienda ha la funzione di affiancare il titolare e i responsabili del trattamento affinché conservino i dati e gestiscano i rischi seguendo i principi e le indicazioni del GDPR. È un consulente dotato di specifica professionalità e delle competenze necessarie per assolvere i compiti che gli sono affidati, in particolare sorvegliare e collaborare alle politiche datoriali in materia di privacy, informare i lavoratori e le organizzazioni sindacali, cooperare con le Autorità.[63]

---

[60] C. Ogriseg, op. cit., pag. 40

[61] A. Ingrao, op. cit., pag. 99-102

[62] A tal fine è fondamentale la previsione dell'articolo 15 lettera f): l'interessato ha diritto di essere informato dell'esistenza nei suoi confronti di un processo decisionale automatizzato ed ha diritto di conoscerne la logica utilizzata e le conseguenze del trattamento dei dati.

[63] C. Del Federico, op. cit., pag. 72

Il suo ruolo è dunque fondamentale nel collaborare a garantire la trasparenza necessaria al rispetto dei diritti dei lavoratori.

Per quanto riguarda l'apparato sanzionatorio, il legislatore europeo ha voluto potenziarlo dando maggiore spazio alle sanzioni di natura amministrativa, con l'introduzione di sanzioni pecuniarie particolarmente elevate che dovrebbero costituire un deterrente all'elusione delle norme; il nuovo assetto valorizza quindi il carattere collettivo e preventivo delle sanzioni amministrative rispetto a quello risarcitorio e individuale del rimedio civilistico.[64]

La nuova impostazione del Regolamento attribuisce infine una notevole importanza alle Autorità Garanti[65], che ricoprono un ruolo fondamentale non solo per i loro rafforzati poteri sanzionatori ma anche in relazione al contributo in fase precauzionale e preventiva, nonché nella promozione dell'adozione di regole deontologiche.[66] Infatti, qualora il tipo di trattamento che prevede l'utilizzo delle nuove tecnologie possa costituire un rischio elevato per i diritti e le libertà delle persone, il titolare è tenuto a porre in essere una specifica valutazione del rischio, a considerare l'opportunità di idonee misure per ridurlo e a consultare l'autorità di controllo, che ha il compito di fornire in merito un parere scritto, indirizzando quindi i comportamenti dei datori di lavoro fornendo indispensabili informazioni e valutazioni, adeguate e aggiornate.

[64] A. Ingrao, op. cit, pag. 144-148

[65] In Italia l'Autorità Garante ha svolto anche precedentemente all'entrata in vigore del Regolamento un'importante attività di precisazione delle disposizioni contenute nel Codice della Privacy elaborando Linee guida e Provvedimenti generali.

[66] C. Ogriseg, op. cit., pag. 56

# CAPITOLO 3

# I DIRITTI DEI LAVORATORI NELLA FASE PREASSUNTIVA E DI SELEZIONE

## 3.1. La fase di reclutamento nel rapporto di lavoro privato

Il primo contatto tra datore di lavoro e lavoratore si stabilisce già nella fase di selezione finalizzata all'assunzione e quindi le possibili discriminazioni possono aver luogo già prima dell'instaurazione del rapporto.

Fino a pochi anni fa il reclutamento del lavoratore avveniva quasi esclusivamente tramite l'analisi delle informazioni acquisite attraverso i curricula pervenuti in azienda, i colloqui di lavoro ed eventualmente l'utilizzo di test attitudinali, che richiedevano notevole competenza e capacità di analisi da parte del reclutatore.

I nuovi mezzi messi a disposizione dalla tecnologia hanno completamente rivoluzionato le modalità con le quali si incontrano domanda e offerta di lavoro. Chi cerca lavoro può utilizzare molteplici canali per visualizzare le offerte presenti sul mercato e può mettere a disposizione il proprio curriculum su siti aziendali e piattaforme dedicate, raggiungendo con pochi click una mole considerevole di potenziali datori di lavoro.

Se le nuove tecnologie danno la possibilità ai lavoratori di inviare capillarmente il curriculum alle aziende, anche i datori di lavoro utilizzano sempre più spesso le nuove tecnologie per far conoscere agli interessati la presenza di eventuali ricerche di personale, non solo attraverso il sito internet aziendale, ma anche con specifiche pagine sui social network, che sono facilmente visualizzabili da una molteplicità di possibili candidati.

Sempre più diffuso è il ricorso ad aziende che si occupano di selezionare il

personale, valutando i curricula pervenuti con strumenti sempre più raffinati.[67]

La quantità di potenziali candidati, aumentata dalla possibilità di inviare capillarmente il proprio curriculum a basso costo utilizzando i canali tecnologici, offre sicuramente maggiori possibilità di mettere in relazione domanda e offerta di lavoro, ma i sistemi di selezione finora utilizzati si possono rilevare inadeguati ad elaborare grandi quantità di proposte; la tecnologia offre nuovi strumenti che possono rivoluzionare le modalità di selezione del personale, con l'introduzione di tecniche di data analysis e algoritmi di machine learning, che rendono le procedure meno complesse e costose.[68]

Gli algoritmi di recruiting permettono di compiere uno screening automatizzato dei CV e di scegliere quelli che più si avvicinano al profilo ricercato, creando un modello di riferimento con tecniche di machine learning che utilizzano le informazioni del personale già in forza in azienda, così da introdurre nell'organizzazione figure professionali simili e creare gruppi di lavoro omogenei. [69]

Tra i metodi più utilizzati l'utilizzo di chabot, con la creazione di job assistant per selezionare gli aspiranti, rispondere in tempo reale alle domande dei candidati riguardanti le posizioni aperte in tempo reale e con esse ottenere feedback che permettono ai chabot stessi di perfezionare le proprie risposte con un processo di machine learning continuo.

---

[67] S. Renzi, *Decisioni automatizzate, analisi predittive e tutela della privacy dei lavoratori*, Lavoro e diritto, Il Mulino Rivisteweb, pag. 5-6

[68]Ad esempio, la piattaforma Ideal offre un assistente virtuale addestrato su uno storico di milioni di decisioni precedenti, identificando velocemente gli elementi desiderati con tecniche di pattern-recognition.

[69]Alcune piattaforme, ad esempio Entelo, analizzano grandi moli di dati per rivolgere il recruiting anche ai soggetti passivi, ovvero lavoratori aperti a nuove possibilità ma che non cercano attivamente un impiego, favorendo la scoperta di candidati qualificati.

L'algoritmo di recruiting è utilizzato anche per effettuare analisi probabilistiche. Infatti, attraverso la raccolta e l'analisi dei big data l'AI elabora un modello predittivo che mira ad individuare in anticipo la probabilità che si verifichi un determinato evento, ad esempio che un candidato ottenga il maggior successo professionale oppure che rassegni presto le proprie dimissioni.

Un ulteriore ambito di applicazione dell'intelligenza artificiale nella selezione del personale riguarda lo studio del comportamento dei candidati tramite l'utilizzo dei dati ricavabili dai social network, con la finalità di profilazione delle soft skills[70]; in quest'ambito l'uso dei dati biometrici può rappresentare un ulteriore possibilità di sviluppo.[71]

L'algoritmo di recruiting in questo caso si occupa di studiare i contenuti pubblicati dal candidato sui social network per ricostruire un profilo psicologico che permetta di verificare le soft skills dichiarate nel CV, che rappresentano sempre più uno degli aspetti fondamentali da tenere in considerazione per la scelta del candidato più adatto al ruolo da ricoprire.[72]

Numerose sono le società che ricorrono ai sistemi automatizzati per la gestione delle candidature, poiché permettono di semplificare notevolmente i processi di gestione e selezionare il personale soprattutto in contesti dove l'offerta di candidati è alta.

Tali sistemi, noti anche con il termine ATS (acronimo di Applicant Tracking System), elaborano i dati presenti nei CV con l'utilizzo di parametri predeterminati e, se le informazioni contenute soddisfano i requisiti stabiliti

[70] M. Forlivesi, *Il controllo della vita del lavoratore attraverso i social network*, in P. Tullini, *Web e* lavoro. Profili evolutivi e di tutela, op. cit., pag. 41

[71] C. Sarra, op. cit., pag. 33

[72]In tale ambito la recente letteratura ha mostrato che le reti neurali convoluzionali possono essere utilizzate per ricostruire i cinque tratti fondamentali di una persona attraverso l'esame delle espressioni facciali estratte da un video, vedi Sarra C., op. cit., pag. 35

dall'algoritmo, i candidati vengono ammessi alla fase successiva della selezione, mentre se il sistema evidenza difformità la candidatura sarà rigettata.[73]

L''utilizzo di questi software pone non pochi problemi dal punto di vista della possibilità di discriminare alcuni lavoratori e della protezione dei dati personali dei candidati.

Emblematico è il caso di Amazon, che tra il 2014 e il 2017 ha costruito un team di esperti di machine learning per la selezione dei candidati attraverso un algoritmo in grado di esaminare i curricula; tale sistema tendeva però a discriminare le donne perché costruito partendo dall'analisi dei dati relativi ai dipendenti in forza alla società nei dieci anni precedenti, che vedeva la netta prevalenza di lavoratori di sesso maschile, con le donne poco rappresentate per figure professionali nell'ambito della tecnologia e che quindi ricevevano dall'algoritmo di selezione un'ingiustificata valutazione inferiore rispetto ai candidati maschi.[74]

L'opacità dell'algoritmo può generare facilmente discriminazioni in base al sesso, all'età o altre caratteristiche dei candidati che nulla hanno a che fare con le competenze e capacità professionali.

Se l'articolo 22 del GDPR pone un importante limite in tal senso[75], vietando le selezioni basate unicamente sull'algoritmo e rendendo quindi necessario

---

[73] Naturalmente potrà accadere che un candidato sia scartato non perché non ha le competenze richieste, ma semplicemente perché il documento non contiene alcuni elementi contenutistici o grafici ritenuti essenziali; affinché il CV non sia scartato per errore è fondamentale quindi che il documento riporti le informazioni con le modalità definite in fase di progettazione, in particolare che siano utilizzata nella descrizione delle competenze la terminologia utilizzata dai programmatori nella definizione delle parole chiave per quella ricerca.

[74] I. Del Giglio, *Valutazione della performance mediante tecniche di People Analytics. Privacy in employment, controllo o innovazione?* in Journal of Ethics and Legal Technologies, vol. 3(2), novembre 2021, pag. 117-118

[75] Così il comma 1 l'art. 22 del GDPR: "*L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.*"

l'intervento umano nei processi di selezione, non impedisce tuttavia che possano avvenire discriminazioni in questa prima fase di scrematura dei curricula, che porta ad escludere parte dei candidati dai successivi colloqui selettivi; in tal senso è determinante che la presenza umana sia attiva anche in questa fase per individuare e correggere eventuali storture determinate da errori di programmazione dell'algoritmo.

L'opacità dell'algoritmo rende, altresì, molto ardua l'individuazione di possibili discriminazioni da parte dei soggetti interessati dato che le modalità con le quali l'intelligenza artificiale giunge a un determinato risultato rimangono per lo più oscure[76] e chi cerca lavoro difficilmente avrà la possibilità di verificare se c'è stata discriminazione ai suoi danni.

Al fine di prevenire eventuali penalizzazioni è importante che i candidati elaborino il proprio curriculum tenendo conto della possibilità che la selezione avvenga tramite sistemi di AI recruiting, così da ottimizzare le informazioni fornite ai fini della particolare selezione alla quale è destinato.

Il curriculum resta uno strumento indispensabile per chi cerca lavoro ed è importante che ci sia da parte del lavoratore la consapevolezza dell'importanza delle indicazioni fornite. Certamente il candidato dovrà evidenziare le competenze professionali e dare tutte quelle informazioni ritenute utili ai fini di essere scelto per la posizione da ricoprire, ma è altrettanto importante essere consapevoli che la scelta della terminologia utilizzata e l'inserimento o meno di talune informazioni anche a carattere personale possono rappresentare la differenza tra un buon curriculum e un curriculum capace di far emergere la propria candidatura tra tutte le altre.

Oltre che alla scrittura del curriculum, particolare attenzione va poi destinata

[76] Si parla in questi casi di black box: il linguaggio di programmazione non permette la comprensibilità delle istruzioni poste a fondamento dell'algoritmo, rendendo di fatto impossibile verificare i criteri utilizzati

alle modalità di utilizzo dei social network. Le persone, infatti, pubblicano foto, notizie, commenti e altri dati e molto spesso manca la consapevolezza dei rischi per la propria privacy nell'utilizzo di tali canali di comunicazione. Il consenso prestato a tali piattaforme è, spesso, frutto di una lettura superficiale dell'informativa e non sempre, nel momento in cui si pubblica una foto o un commento che veicola una propria opinione, ci si rende contro che tali informazioni sono messe a disposizione di un vasto pubblico, che può comprendere anche un datore di lavoro presente o futuro.

È quindi importante utilizzare i canali comunicativi in modo corretto e consapevole, scegliendo, al momento dell'inserimento, una visualizzazione aperta a chiunque o ristretta agli "amici". Il conseguente trattamento di dati è ben diverso dato che se si sceglie la prima opzione si dovrà avere la consapevolezza che anche il datore di lavoro (o il futuro datore di lavoro) potrà avere libero accesso a tali informazioni, mentre se si sceglie la modalità ristretta, sarà possibile poi contestare al datore di lavoro, che riesca ad accedervi attraverso altri canali, l'utilizzo di dati che non erano nella sua disponibilità.[77]

In conclusione, la corretta informazione rispetto ai propri diritti è fondamentale per poter salvaguardare la propria privacy: se l'utilizzo delle nuove tecnologie rappresenta per gli utenti un notevole vantaggio nel processo che mette in relazione domanda e offerta di lavoro, è necessario che tutti gli attori di tale processo abbiano la consapevolezza dei potenziali rischi sotto il profilo della riservatezza.

## 3. 2. La selezione nella pubblica amministrazione

La trasformazione digitale che sta coinvolgendo la Pubblica Amministrazione

[77] M. Forlivesi, op. cit, pagg. 40-42

ha portato all'introduzione degli algoritmi anche nell'istruttoria di procedure tradizionalmente condotte da funzionari specializzati. L'uso delle nuove tecnologie da parte della Pubblica Amministrazione non può in ogni caso comportare l'attenuazione degli obblighi di trasparenza e motivazione dei provvedimenti amministrativi; il complesso rapporto tra algoritmi della pubblica amministrazione e trasparenza è oggetto di analisi specifiche.[78]

Come è noto, l'accesso al pubblico impiego avviene, ai sensi dell'articolo 97 della Costituzione, tramite concorso pubblico, differenziandosi quindi notevolmente dalle modalità di selezione precedentemente illustrate per il settore privato, anche se, come vedremo, possono anche in questo caso verificarsi discriminazioni ai danni dei candidati.[79]

L'intelligenza artificiale applicata alla Pubblica Amministrazione può rappresentare la chiave per modernizzare il processo di selezione del personale; l'articolo 1 del nuovo regolamento per le assunzioni nel pubblico impiego ( DPR n. 82 del 16 giugno 2023), che ha riformato il DPR n. 487 del 9 maggio 1984, a tal fine stabilisce che "i*l concorso pubblico si svolge con modalità che ne garantiscano l'imparzialità, l'efficienza, l'efficacia nel soddisfare i fabbisogni dell'amministrazione reclutante e la celerità di espletamento ricorrendo, ove necessario, all'ausilio di sistemi automatizzati diretti anche a realizzare forme di preselezione e a selezioni decentrate per circoscrizione territoriali."*

Nell'ambito delle selezioni pubbliche, l'uso di algoritmi e di procedure automatizzate può essere assimilato a tutti gli effetti a un "atto amministrativo informatico" che deve necessariamente sottostare a principi di ragionevolezza, proporzionalità, pubblicità e trasparenza.

---

[78] G. Ragone, *Gli algoritmi e l'attività amministrativa*, 9 aprile 2020 (https://www.filodiritto,com)

[79]La valutazione automatica delle prove scritte, attraverso un algoritmo che utilizzava per la correzione determinate parole chiave, ha generato ricorsi da parte dei candidati, che hanno ritenuto discriminante e non trasparente la modalità di valutazione.

Esistono certamente vincoli etici, tecnici, giuridici, organizzativi che limitano l'adozione diretta e generalizzata dell'Intelligenza artificiale, in particolare l'articolo 22 del GDPR[80].

La giurisprudenza ritiene ammissibili e anzi auspicabili algoritmi di ausilio all'attività amministrativa, che supportano le decisioni umane nell'elaborazione di grandi moli di dati processando istruzioni umane routinarie, ma ritiene incompatibili decisioni autonome dell'IA, fondate su algoritmi di Deep Learning, in cui la scelta si fonda su un percorso logico non ricostruibile.

In tal senso fondamentale importanza rilevano due sentenze del Consiglio di Stato del 2019, la n. 2270 e la n. 8472, che si pronunciano in merito ad altrettante sentenze del Tar del Lazio.

La sentenza n. 2270/2019 riguarda il ricorso di alcuni docenti della scuola secondaria di secondo grado contro la procedura di selezione utilizzata per l'attribuzione della classe di concorso e della sede di destinazione nell'ambito del piano straordinario nazionale di cui alla legge n. 107/2015.

I ricorrenti lamentavano che l'intera procedura di assunzione era stata affidata a un sistema informatico per mezzo di un algoritmo, il cui meccanismo sarebbe rimasto sconosciuto, ed era sfociata in provvedimenti privi di motivazione, senza l'individuazione di un funzionario incaricato di seguire e controllare l'intero procedimento.

I giudici sottolineano come sia fondamentale la digitalizzazione dell'amministrazione pubblica, che può garantire un miglioramento dei servizi resi ai cittadini e agli utenti; l'automazione del processo decisionale dell'amministrazione mediante l'utilizzo di una procedura digitale e

[80] Vedi sentenza n. 8472/2020 del Consiglio di Stato, che ha sancito la non esclusività della decisione algoritmica

attraverso l'algoritmo, in particolar modo con riferimento a procedure seriali o standardizzate, è infatti "conforme ai canoni di efficienza ed economicità dell'azione amministrativa, ai sensi dell'articolo 1 della Legge 241/1990, i quali, secondo il principio costituzionale di buon andamento dell'azione amministrativa (art. 97 Cost.), impongono all'amministrazione il conseguimento dei propri fini con il minor dispendio di mezzi e risorse e attraverso lo snellimento e l'accelerazione dell'iter procedimentale."

L'utilizzo di procedure informatiche va quindi incoraggiato e non stigmatizzato, ma deve essere effettuato nel rispetto dei principi che regolano lo svolgimento dell'attività amministrativa.[81]

L'algoritmo utilizzato deve essere conoscibile in tutti i suoi aspetti, al fine di poter verificare che gli esiti del procedimento siano conformi alle prescrizioni e alle finalità stabilite dalla legge o dalla stessa amministrazione e siano chiare le modalità e le regole con le quali è stato impostato.

La regola algoritmica deve essere non solo conoscibile in sé, ma anche soggetta alla piena cognizione e al pieno sindacato del giudice amministrativo.

I giudici hanno quindi accolto l'appello, ritenendo violati i principi di imparzialità, pubblicità e trasparenza, valutando l'impossibilità di comprendere le modalità di assegnazione tramite l'algoritmo come un vizio in grado di inficiare l'intera procedura.

La successiva sentenza n. 8472 del 13 dicembre 2019 riguarda anch'essa la procedura algoritmica utilizzata nell'ambito del piano straordinario di assunzioni di cui alla Legge n. 107/2015, in particolare quella utilizzata per decidere i trasferimenti dei docenti a sede diversa da quella di prima assegnazione.

---

[81] G. Resta, *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, Politica del diritto, Fascicolo 2, giugno 2019, Il Mulino, pag. 213

I giudici richiamano quanto già espresso nella sentenza n. 2270/2019, sottolineando l'importanza di ricorrere a procedure informatizzate al fine di ottenere una maggiore efficienza ed efficacia della Pubblica Amministrazione attraverso lo snellimento e l'accelerazione dell'iter procedimentale; tuttavia, tale utilizzo "non può essere motivo di elusione dei principi che conformano il nostro ordinamento e che regolano lo svolgersi dell'attività amministrativa".
I giudici sottolineano i due aspetti fondamentali che rappresentano i criteri minimi di garanzia per l'utilizzo di algoritmi in sede decisoria pubblica: la piena conoscibilità del modulo utilizzato e dei criteri applicati e l'imputabilità della decisione all'organo titolare del potere.
La conoscibilità dell'algoritmo deve essere garantita in tutti i suoi aspetti e non può assumere rilievo l'invocata riservatezza delle imprese produttrici dei meccanismi informatici utilizzati, le quali devono necessariamente accettare le conseguenze in termini di trasparenza del porre al servizio della Pubblica Amministrazione tali strumenti.
La sentenza individua quindi i tre principi che emergono dall'analisi del diritto sovranazionale[82] e devono necessariamente essere rispettati nel caso di utilizzo degli strumenti informatici: il principio di conoscibilità, il principio di non esclusività della decisione algoritmica (art. 22 del GDPR) e il principio di non discriminazione algoritmica[83].
La Corte ritiene quindi che non deve ritenersi applicabile alla decisione algoritmica l'intera disciplina della L. 231/1990, ma è necessario che siano resi noti i criteri con cui opera l'algoritmo e che sia definito un centro di imputabilità (soggetto fisico) se si verifica una fallacia.
La corretta applicazione dei principi ricavabili dalla normativa permetterebbe

[82] In particolare, vedi artt. 13, 14 e 15 del GDPR
[83] Vedi considerando n. 71 del GDPR 679/2016

così di guardare con favore all'innovazione tecnologica anche nella Pubblica Amministrazione, perseguendo l'obiettivo del buon andamento e imparzialità dell'azione amministrativa riscontrabile nel dettato costituzionale.

Il principio di conoscibilità della decisione algoritmica è ribadito nella sentenza n. 730/2020 del Tar del Lazio, intervenuta sull'istanza di accesso agli atti formulata da alcuni aspiranti dirigenti scolastici che avevano partecipato a una prova selettiva gestita tramite software.

Il Tar ha ammesso l'accesso all'intero codice sorgente del software utilizzato per la selezione, in quanto solo esso permette di conoscere l'effettivo funzionamento del sistema informatico utilizzato e quindi solo in questo modo è possibile garantire la trasparenza dell'azione della Pubblica Amministrazione.

# CAPITOLO 4

# LA VALUTAZIONE DEL DIPENDENTE NEL MONDO DEL LAVORO DIGITALE

## 4.1. La valutazione della performance e la People Analytics

Le modifiche al mondo del lavoro introdotte dalla digitalizzazione interessano anche la gestione delle risorse umane, con l'automazione dei processi decisionali e delle tecniche di valutazione della performance.

La valutazione della performance dei lavoratori si pone l'obiettivo di misurare le prestazioni svolte dai lavoratori in relazione alla pianificazione degli obiettivi operata dalla direzione aziendale.

Non si tratta di valutare semplicemente il corretto adempimento della prestazione, ma di verificare attitudini e capacità dei gruppi di lavoratori o dei singoli collaboratori con riferimento alle attitudini ma anche ai comportamenti tenuti all'interno dell'organizzazione, che sono espressione del coinvolgimento e attaccamento alla realtà aziendale.

Interpretare i comportamenti e le attitudini è un compito complesso, che il manager tradizionalmente perseguiva attraverso l'osservazione diretta dei lavoratori ma anche con questionari e colloqui; anche se tale valutazione può essere accurata, ha il limite della soggettività del valutatore, che ha il compito di interpretare i dati dell'indagine, ma anche del lavoratore, che in tale contesto può essere influenzato dall'emotività oppure può deliberatamente modificare le proprie risposte e i propri atteggiamenti per adeguarli alle aspettative del valutatore.[84]

Con la digitalizzazione del lavoro, anche per la valutazione della performance

[84] I. Del Giglio, op.cit., pag. 104-106

sono disponibili nuovi strumenti e nuove tecniche, che permettono di codificare le prestazioni tramite l'analisi di grandi quantità di dati generati dai dispositivi tecnologici; si aggiungono inoltre nuovi elementi e parametri di valutazione, figli delle nuove realtà organizzative e produttive generate dalle innovazioni tecnologiche e dall'utilizzo dell'IA nei sistemi produttivi e finalizzati a individuare quei comportamenti innovativi che possono rappresentare un *plus* nella performance del lavoratore.

La tecniche di People Analytics, definibili come la "*raccolta e analisi di grandi quantità di dati per identificare modelli di atteggiamento e prevedere comportamenti di gruppi e comunità*" rappresentano una vera e propria rivoluzione anche nell'ambito della gestione delle risorse umane (in tale ambito è usata la definizione di HR Analytics): l'uso di tali tecniche dovrebbe permettere di selezionare il miglior candidato, promuovere il miglior dipendente, costruire il team più efficace e individuare il lavoratore improduttivo, indirizzando le strategie di gestione elaborate dai manager.[85]

Le fonti della raccolta dei Big data utilizzati con tali tecniche sono eterogenee. A titolo di esempio si ricordano le videocamere, i social network, le banche dati contenenti le informazioni sui lavoratori (definite con l'acronimo HRIS, Human Resources Information System) e le banche dati contenenti i dati dei clienti (dette CRM, Costumer Relationship Management) ma utilizzabili anche per ottenere informazioni indirette sui lavoratori, i Digital workplace (spazi di lavoro digitali con piattaforme sulle quali viene svolta l'attività lavorativa ma che consentono anche dinamiche relazionali tra i dipendenti e l'organizzazione).

Le analisi effettuate possono avere finalità descrittive, ovvero verificare cosa

[85] E. Dagnino, *People Analytics: lavoro e tutele al tempo del management tramite big data*, LLI, vol. 3, n. 1, 2017, pag. 8

effettivamente accade in azienda, oppure diagnostiche o predittive, indirizzate a capire come evolverà la situazione e quali misure sono necessarie per risolvere o prevenire i problemi organizzativi.

Non esistono norme specifiche che regolano l'utilizzo della People Analitycs, le fonti richiamabili sono quelle nazionali e internazionali già citate, che definiscono i diritti fondamentali dei lavoratori e vanno attentamente analizzate per verificare il confine tra valutazione della performance e controllo occulto.[86]

Tali procedure di analisi automatizzate saranno infatti sempre più utilizzate anche per gestire le risorse umane, ma è importante che siano correttamente rilevate le criticità che possono generare.

Necessariamente dobbiamo richiamare la difficoltà di distinguere tra strumenti di lavoro e strumenti di controllo, aggravata dall'utilizzo promiscuo dei dispositivi e dall'introduzione di nuove tecnologie quali i dispositivi IoT e wearable, largamente utilizzati soprattutto nel campo della sicurezza.

I rischi per i diritti dei lavoratori sono riferibili al trattamento dei dati, che può essere occulto, pervasivo, abnorme e impersonale; se anche la forma di acquisizione può essere neutra, l'elaborazione dei dati può dare luogo a controlli viziati e a discriminazioni indirette, con l'utilizzo di un criterio neutro che però può generare una situazione di svantaggio per uno o più lavoratori.[87]

Altri rischi possono derivare dall'utilizzo stesso dello strumento informatico: i sistemi di Intelligenza Artificiale sono costituiti da una rete neurale convoluzionale, che risulta difficilmente comprensibile per l'oscurità dei meccanismi che regolano le sue decisioni nonché per la sua complessità tecnica. Tale meccanismo può portare a conclusioni viziate, che possono essere

[86] I. Del Giglio, op.cit., pag. 120-121

[87] E. Dagnino, op. cit., pag. 22-24

imprevedibili e non intenzionali ma anche effetto della volontà di chi ha programmato l'algoritmo, con la possibile generazione di discriminazione diretta (nel caso in cui il modello è volontariamente costruito per escludere una determinata categoria di persone) oppure indiretta (quando il modello è costruito in modo neutro ma i processi decisionali conseguenti generano comunque un impatto diverso su alcuni soggetti).

L'utilizzo improprio di tecniche di HR Analytics può generare un esercizio occulto del potere di controllo, può influire sulla valutazione della performance del lavoratore e condurre a inesistenti responsabilità disciplinari, oppure all'adozione nei suoi confronti di trattamenti peggiorativi, discriminatori o ritorsivi.[88]

I big data rappresentano quindi una sfida, un'opportunità ma anche un rischio. Infatti, l'utilizzo delle tecniche di analisi è certamente funzionale ai nuovi bisogni delle organizzazioni; tuttavia, per il rispetto dei diritti fondamentali dei lavoratori è indispensabile porre particolare attenzione alla creazione di modelli di valutazione che ottemperino alle limitazioni poste dalle norme a tutela dei diritti dei lavoratori.

Innanzitutto, le tecniche di People Analytics dovrebbero essere utilizzate come supporto e non in sostituzione dell'intervento umano, nel rispetto di quanto indicato all'articolo 22 del GDPR, pertanto il manager potrà servirsi dell'IA quale ausilio per analizzare le soft skills e giungere ad una decisione informata.

Altro aspetto fondamentale è la trasparenza e comprensibilità del procedimento utilizzato, che renda intellegibili le decisioni assunte per poterne verificare la correttezza e che prenda in considerazione solo i dati

[88] I. Del Giglio, op.cit., pag. 116-120

realmente rilevanti per la finalità perseguita.[89]

Risulta fondamentale il rispetto dell'articolo 8 dello Statuto dei lavoratori, sia nella fase di raccolta dei dati che all'esito della fase di analisi, che attraverso i meccanismi di correlazione applicati può generare nuova conoscenza.[90] In tale contesto l'articolo 8 può generare difficoltà interpretative con riferimento all'estensione del divieto ai fatti non rilevanti ai fini della valutazione dell'attitudine professionale, dato che nell'attività di People Analytics non sempre è facile individuare il collegamento che ci deve essere tra il fatto oggetto di indagine e l'accertamento dell'attitudine professionale, mancando in tali ipotesi il meccanismo causa-effetto alla base delle tecniche di indagine tradizionali e, anzi, risultando perlopiù oscuro il meccanismo di correlazione utilizzato.

La fase di decisione può essere influenzata da errori compiuti in fase di costruzione del modello, oppure nella raccolta dei dati trattati o per l'inserimento di criteri discriminatori, voluti o meno. Per un utilizzo consapevole di tali strumenti, indispensabile si rivela la formazione dei manager, che devono conoscere e comprendere modalità di utilizzo e possibili rischi insiti in tali tecnologie.

Per un utilizzo consapevole e conforme alla riservatezza dei lavoratori l'attenzione deve necessariamente spostarsi alla fase di programmazione degli strumenti, ove i principi di privacy by design privacy by default contenuti nel

---

[89] M. Peruzzi, *Il diritto antidiscriminatorio al test dell'intelligenza artificiale*, LLI, vol. 7, n.1, 2021, pag. 55

[90] Le potenzialità e i rischi generabili dall'analisi di una notevole quantità di dati sono intuibili valutando ad esempio gli esiti di un'indagine sui consumi effettuata da un supermercato americano (vedi E. Dagnino, op. cit., pag. 20): l'analisi dei prodotti acquistati ha permesso di individuare le persone ai primi mesi di gravidanza e la successiva attività di promozione si è rivelata lesiva della privacy di una ragazza minorenne che in tal modo ha visto resi edotti i genitori sul suo stato di gravidanza. Tale esempio ci permette di capire quali conseguenze potrebbe avere l'analisi di imponenti quantità di dati dei lavoratori per finalità di predizione e conoscenza di aspetti anche sensibili e potenzialmente discriminatori.

Regolamento Europeo per la protezione dei dati personali possono rappresentare le linee guida per assicurare l'affidabilità dei modelli utilizzati ed impedire decisioni discriminatorie.

Il coinvolgimento dei lavoratori e dei loro rappresentanti già in questa fase potrebbe infine generare una condivisione positiva, capace di orientare l'utilizzo delle nuove tecniche di People Analytics all'incremento produttivo ma anche al miglioramento delle condizioni dei lavoratori.

## 4.2 La valutazione del lavoratore per l'attribuzione di premialità

La valutazione del prestatore di lavoro assume rilevanza per il lavoratore in relazione all'erogazione di premi di produttività o altri meccanismi incentivanti, quali ad esempio promozioni o adeguamento delle mansioni. I premi di produzione collegati al rendimento sono generalmente previsti da appositi contratti integrativi, ma nulla vieta che nel rapporto di lavoro privato[91] siano adottati meccanismi incentivanti senza che vi sia alla base un accordo collettivo.

La giurisprudenza ha evidenziato come la previsione di un premio collegato al rendimento da un lato esclude la possibilità di un meccanismo di attribuzione automatica, dall'altro comporta che il potere del datore di lavoro sia procedimentalizzato.[92]

Va inoltre ricordato come la retribuzione incentivante non sia d'altra parte un diritto del lavoratore, perché si colloca al di sopra della previsione della retribuzione minima e quindi non fa parte della retribuzione proporzionata e

[91]Nel pubblico impiego sono previste regole specifiche: la Legge n. 150/2009 (Riforma Brunetta) ha introdotto il cosiddetto ciclo di gestione della performance, con finalità di valutazione e premialità dei dipendenti pubblici, poi riformata dalla Legge n. 74/2017 (Riforma Madia)

[92] A. Topo, *Automatic management, reputazione del lavoratore e tutela della riservatezza*, Lavoro e diritto, fascicolo 3, estate 2018, pag. 461

sufficiente garantita dall'articolo 36 della Costituzione.

La valutazione del dipendente con finalità premiali non è quindi necessaria per la gestione del rapporto di lavoro; in tal senso è sufficiente l'accertamento dell'esecuzione della prestazione con la diligenza richiesta dalla natura della prestazione e in caso di inadempimento rispetto alla prestazione secondo i canoni di diligenza considerati standard può verificarsi il licenziamento del lavoratore per scarso rendimento.

I contratti collettivi integrativi possono comunque costituire un valido sistema per introdurre regole e criteri di valutazione da applicare per l'attribuzione dei meccanismi premiali incentivanti che siano trasparenti e condivisi.[93]

## 4.3. La valutazione del lavoratore nei mercati digitali

La valutazione del lavoratore assume rilevanza ancora maggiore ai fini della tutela dei lavoratori nei contesti lavorativi fortemente influenzati dall'applicazione delle tecnologie informatiche, dove l'attività di management è divenuta totalmente automatizzata. Ci si riferisce all'ipotesi in cui una piattaforma elettronica svolge le funzioni di datore di lavoro, attribuendo le mansioni e i carichi di lavoro e controllando la qualità della prestazione attraverso l'algoritmo.[94]

La valutazione della prestazione dei lavoratori in tali contesti può coinvolgere anche i fruitori dei servizi; a metodi tradizionali di rilevazione della costumer satisfaction, quali questionari di gradimento o moduli di reclamo, si affiancano o sostituiscono sistemi di valutazione digitalizzati, con la possibilità di raccogliere informazioni dagli utenti in modo rapido ed efficace.

---

[93] A. Topo, ivi. Pag. 462

[94] L. Zappalà, *Informatizzazione dei processi decisionali e diritto del lavoro: algoritmi, poteri datoriali e responsabilità del prestatore nell'era dell'intelligenza artificiale*, Biblioteca 20 maggio, 2/2021, pag. 112-114

Tali meccanismi possono però influire significativamente sulla carriera dei lavoratori che operano in questi settori. I giudizi degli utenti sono utilizzati per misurare l'adeguatezza delle prestazioni offerte dalla piattaforma ma di conseguenza anche l'attitudine dei lavoratori a soddisfare le loro richieste, che si traducono in un punteggio che l'automatic management utilizzerà poi per assumere decisioni strategiche finalizzate ad aumentare la fiducia e la reputazione della piattaforma, attraverso la creazione dell'incontro ottimale tra domanda e offerta.[95]

L'adozione di tali sistemi di valutazione permette quindi agli utenti di esprimere giudizi e preferenze sul lavoro svolto dagli operatori, che si trovano così ad essere valutati da soggetti terzi.

L'affidamento della valutazione dei lavoratori a soggetti diversi dal datore di lavoro può avvenire e avviene anche nelle forme di lavoro tradizionali, in particolare da imprese di servizi specializzate in attività di selezione e valutazione.

Nel caso della valutazione degli utenti possono però assumere rilevanza notevole i possibili atteggiamenti potenzialmente discriminatori degli utenti, che non operano professionalmente e che possono generare giudizi condizionati ad esempio dal sesso o dall'appartenenza etnica del prestatore di lavoro.

Se tali valutazioni sono poi utilizzate per produrre decisioni sulla distribuzione delle occasioni lavorative, la reputazione del lavoratore che da esse è generata può rappresentare un meccanismo premiante ma anche di penalizzazione, che pone i lavoratori in constante confronto tra di loro e ne determina le maggiori o minori opportunità lavorative.

Si rivela quindi indispensabile l'adozione di regole che rendano trasparenti le

[95] A. Topo, op. cit., pag. 457-459

modalità di valutazione, al fine di consentire al lavoratore di verificare la corretta applicazione e il rispetto dei propri diritti.

Va inoltre sottolineato come la valutazione della piattaforma tramite la valutazione del lavoratore determina anche lo spostamento del rischio economico: è il prestatore di lavoro, infatti, attraverso il profilo reputazionale costruito tramite i giudizi degli utenti, a subire le conseguenze economiche di tale valutazione, che si palesa con la maggiore o minore attribuzione di possibilità lavorative, fino a giungere all'esclusione dalla piattaforma, cioè a un licenziamento svincolato dai limiti di legge.[96]

La reputazione del lavoratore costruita attraverso tali meccanismi di valutazione dovrebbe poi poter essere valorizzata non solo all'interno della piattaforma nella quale opera, ma anche contribuire alla costruzione di un profilo professionale che permetta al prestatore di lavoro di spendere il riconoscimento delle proprie capacità e competenze da parte degli utenti anche presso altri potenziali datori di lavoro, favorendo quindi il trasferimento da una piattaforma ad un'altra e la possibilità di migliorare la propria posizione lavorativa.[97]

[96] L. Zappalà, op. cit, pag. 114

[97] A. Topo, op. cit. pag.470-473

# CONCLUSIONI

La digitalizzazione del mondo del lavoro connessa alle innovazioni della quarta rivoluzione industriale comporta per i lavoratori nuove opportunità ma indubbiamente anche notevoli rischi per i diritti fondamentali della persona, con nuovi pericoli per la dignità e la riservatezza.

L'evoluzione tecnologica ha certamente una velocità di sviluppo che rende difficile per il legislatore tenere il passo, anche se le recenti innovazioni introdotte a livello europeo e nazionale hanno indubbiamente contribuito ad adeguare le tutele.

In materia di protezione dei dati personali il nuovo Regolamento europeo n. 769/2016 ha contribuito a dare un profilo sovranazionale ed uniforme alle norme poste a salvaguardia del fondamentale diritto alla riservatezza dei cittadini e dei lavoratori, con una nuova impostazione programmatica che mira a prevenire i possibili illeciti con misure di privacy by design e privacy by default, che responsabilizzano i titolari del trattamento e permettono agli interessati di diventare soggetti attivi del trattamento attraverso l'esercizio dei diritti loro attribuiti.

A livello nazionale indubbiamente un ruolo notevole in tal senso va riconosciuto all'articolo 8 dello Statuto dei lavoratori e alla riforma dell'art. 4, che ha permesso di risolvere alcune delle criticità interpretative già rilevate dalla giurisprudenza in merito alla selezione dei dati trattabili e ai controlli tramite i nuovi strumenti digitali, che sono divenuti ormai fondamentali per lo svolgimento dell'attività economica.

L'analisi della normativa, della giurisprudenza e dei provvedimenti dell'autorità garante hanno evidenziato come il legislatore ponga sempre al centro il bilanciamento degli interessi delle parti, mirando a salvaguardare le necessità del datore di lavoro di perseguire le proprie finalità imprenditoriali,

ottimizzando l'utilizzo delle nuove tecnologie anche per la gestione delle risorse umane, ma nel rispetto dei diritti dei lavoratori costituzionalmente tutelati.

La digitalizzazione ha evidenziato notevoli possibilità di impiego anche nel campo della gestione e valorizzazione delle risorse umane. Infatti, le nuove tecniche di Data Analysis possono portare notevoli opportunità di innovazione e miglioramento anche per il management, con applicazioni di portata straordinaria sia nel campo della selezione sia della valutazione del personale, che possono generare vantaggi notevoli per datori di lavoro e lavoratori, ma che richiedono anche particolare attenzione per evitare discriminazioni e abusi.

Il rispetto dei principi che il Regolamento Europeo e le altre norme sovranazionali, nonché le fondamentali tutele poste in essere dallo Statuto dei lavoratori sembrano costituire una solida base di protezione se rigidamente applicati. Tuttavia, l'impatto dirompente dell'utilizzo dell'intelligenza artificiale in tutti i settori genera nuove perplessità e la consapevolezza della necessità di un continuo adeguamento della legislazione in materia.

In tal senso il legislatore comunitario ha avvertito l'esigenza di predisporre una serie di interventi di rinnovamento della legislazione vigente, tra i quali assumono particolare rilievo il Libro bianco sull'intelligenza artificiale pubblicato il 19 febbraio 2020, che si pone l'obiettivo di promuovere la diffusione dell'utilizzo dell'Intelligenza Artificiale e di affrontare i rischi che discendono dal suo utilizzo, e la proposta di Regolamento del Parlamento Europeo e del Consiglio presentata il 21 aprile 2021, che porterebbe alla regolamentazione dei vari aspetti della materia a livello sovranazionale con un provvedimento self-executing per gli Stati membri.

Notevole rilevanza assume anche la proposta di direttiva per migliorare le

condizioni del lavoro mediante piattaforme digitali presentata alla Commissione Europea il 9 dicembre 2021, che rappresenta un passo avanti anche per il rafforzamento delle prerogative sindacali in quanto all'art. 9 introduce in capo alle piattaforme un obbligo di informazione e consultazione dei rappresentanti dei lavoratori, per "decisioni che possono comportare l'introduzione o modifiche sostanziali nell'uso di sistemi decisionali e di monitoraggio autorizzativo".

Si aggiunge infine al quadro normativo europeo la Proposta di risoluzione del Parlamento Europeo del 3 maggio 2022 e la proposta di Direttiva sul diritto alla disconnessione allegata alla risoluzione del Parlamento Europeo del gennaio 2021.

Le rivoluzionarie trasformazioni economiche e sociali che la diffusione delle nuove tecnologie dell'era digitale stanno provocando costituiscono quindi una notevole sfida per il diritto del lavoro, che è chiamato a cercare di stare al passo con cambiamenti continui e imprevedibili per poter garantire anche ai lavoratori dell'Industria 4.0 la tutela dei diritti fondamentali.

Da più parti si evidenzia la necessità di un intervento legislativo anche a livello nazionale, con una revisione dello Statuto dei lavoratori che vada oltre la riforma operata nel 2015, intercettando le nuove esigenze del mondo del lavoro e rafforzando il ruolo della contrattazione.

# **BIBLIOGRAFIA**:


Ambrosino A., *Riflessioni sul potere datoriale di controllo alla luce delle pronunce della Corte europea dei diritti dell'uomo sul caso Bărbulescu c. Romania*, Variazioni su temi di diritto del lavoro, fascicolo 1/2018

Aimo M., *Dalle schedature dei lavoratori alla profilazione tramite algoritmi: serve ancora l'art. 8 dello Statuto dei lavoratori?*, Lavoro e diritto, a. XXXV, n. 3-4, estate autunno 2021

Barraco E, *Privacy del lavoratore e controlli tecnologici*, Diritto e pratica del lavoro, 40/2016

Busia G., *Così vicini, così distanti: i controlli da remoto del datore di lavoro e la riservatezza del dipendente*, Lavoro Diritti Europa, 3/2020

Cairo L, Villa U., *I controlli a distanza a quattro anni dal Jobs Act*, Il lavoro nella giurisprudenza 7/2019

Dagnino E., *People Analytics: lavoro e tutele al tempo del management tramite big data*, LLI, vol. 3, n. 1, 2017

Del Giglio I., *Valutazione della performance mediante tecniche di People Analytics. Privacy in employment, controllo o innovazione?*, Journal of Ethics and Legal Tecnologies, Volume 3 (2), 11/2021

Ingrao A., *Il controllo a distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata*, Cacucci Editore, Bari, 2018

Lambertucci P., *I poteri del datore di lavoro nello Statuto dei lavoratori dopo l'attuazione del c.d. Jobs Act del 2015: primi spunti di riflessione*, in ADL 3/2016

Lucifora C., *Quale statuto per i lavoratori del XXI secolo?*, in Economia & Lavoro, Fascicolo 1, gennaio-aprile 2021, Il Mulino

Marrazza M., *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore)*, ADL 3/2016

Ogriseg C., *Il regolamento UE n. 2016/679 e la protezione dei dati personali nelle dinamiche giuslavoristiche: la tutela riservata al dipendente*, in Labour and Law Issues, vol 2, n. 2, 2016

Peruzzi M., *Il diritto antidiscriminatorio al test dell'intelligenza artificiale*, Labour & Law Issues, volume 7, 1/2021

Rabai B., *I big data nell'ecosistema digitale: tra libertà economiche e tutela dei diritti fondamentali*, Amministrare, Fascicolo 3, dicembre 2017, Il Mulino

Rausei P., *Controllo a distanza: installazione e uso dei sistemi di geolocalizzazione*, in Diritto e pratica del lavoro, 1/2017

Resta G., *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di eguaglianza*, Politica del diritto, Fascicolo 2, giugno 2019

Renzi S, *Decisioni automatizzate, analisi predittive e tutela della privacy dei lavoratori*, Lavoro e Diritto, Il Mulino

Sarra C., *L'uso di dati biometrici nelle procedure di reclutamento al lavoro mediante strumenti di Intelligenza Artificiale. Difficoltà normative multilivello*, Journal of Ethics and Legal Tecnologies, Volume 4 (2), 11/2022

Sitzia A., *I controlli a distanza dopo il Jobs Act e la Raccomandazione R(2015)5 del Consiglio d'Europa*, Il lavoro nella giurisprudenza 7/2015

Sitzia A., *Personal computer e "controlli tecnologici" del datore di lavoro nella giurisprudenza*, ADL 3/2017

Tebano Laura, *Employees' Privacy and employers' control between the Italian legal system and European sources*, LLI, vol. 3, 2017

Topo A, *"Automatic management", reputazione del lavoratore e tutela della riservatezza*, Lavoro e diritto, Lavoro e diritto, Fascicolo 3, estate 2018

Treu T., *Cinquanta anni di Statuto, e oltre*, Economia & Lavoro, Fascicolo 1, gennaio-aprile 2021

Treu T., *La digitalizzazione del lavoro: proposte europee e piste di ricerca*, in

Federalismi.it, 03/2022

Tufo M., *Potere di controllo datoriale vs. privacy del lavoratore: alla ricerca delle coordinate di ammissibilità dei controlli occulti*, Studium Iuris 7-8/2020

Tullini P. (a cura di), *Web e lavoro. Profili evolutivi e di tutela*, Giappichelli Editore, 2017

Tullini P. (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Giappichelli Editore, 2017

Zappalà L., *Informatizzazione dei processi decisionali e diritto del lavoro: algoritmi, poteri datoriali e responsabilità del prestatore nell'era dell'intelligenza artificiale*, Biblioteca "20 maggio", 2/2021

## SITOGRAFIA:

www.agendadigitale.eu

www.altalex.com

ww.dejure.it

www.eige.europa.eu

www.federalismi.it

ww.filodiritto.it

www.garanteprivacy.it

www.ilsole24ore.com

www.labourlaw.unibo.it

www.lavorodirittieuropa.it

www.smartius.it

www.rivistaianus.it