UNIVERSITÀ DI MODENA E REGGIO EMILIA
FONDAZIONE MARCO BIAGI

Dottorato di ricerca in Lavoro, Sviluppo e Innovazione
Ciclo XXXV

POTERE DATORIALE DI CONTROLLO, GESTIONE ALGORITMICA E TUTELA DELLA RISERVATEZZA DEI LAVORATORI

Candidata: Dott.ssa Ilaria Del Giglio

Relatore: Chiar.mo Prof. Simone Scagliarini
Correlatore: Chiar.mo Prof. Iacopo Senatori

Coordinatrice del Corso di Dottorato: Chiar.ma Prof.ssa Ylenia Curzi

Sintesi

Il presente studio si propone di indagare l'evoluzione del potere di controllo datoriale in relazione alle nuove tecnologie impiegate nei rapporti di lavoro.
La ricerca si concentrerà sul modo di esercitare il potere di controllo in contesti lavorativi integralmente digitali e sulle tutele riconosciute ai lavoratori che operano in tali ambiti per una duplice ragione.
In primo luogo, perché il potere di controllo, divenuto tecnologico, si rafforza dotandosi di nuove abilità che consentono di accedere a informazioni originariamente ignote.
Ciò non solo in ragione degli strumenti innovativi impiegati, ma anche (e soprattutto) per la tipologia di dati acquisibili.
Quest'ultimi, infatti, possono essere caratterizzati da una "non autoevidenza" risultando non immediatamente comprensibili. Da qui la necessità di una fase di elaborazione che li renda intellegibili, operazione che pone il datore di lavoro nella condizione di accedere a nuove informazioni sui lavoratori.
Grazie alla digitalizzazione, dunque, il potere di controllo si dilata in maniera proporzionale alle informazioni che possono essere ottenute da questi "*raw data*".
Le potenzialità cognitive della nuova tecnologia, in ragione delle capacità di archiviazione ed elaborazione, possono così mutare dati originariamente "neutri" in informazioni capaci di incidere sulla condizione dei lavoratori.
In secondo luogo, perché il potere di controllo, abilitato a nuove potenzialità, modifica la propria natura travalicando la tradizionale divisione tra poteri datoriali.
I nuovi strumenti digitali, rispetto alla tecnologia precedente, non intervengono solo nel momento di esecuzione della prestazione, ma ampliano il tempo di utilizzo. Ciò consente di variare il periodo di accesso alle informazioni, anticipandolo o posticipandolo, interferendo sulla fase decisionale e – conseguentemente - sull'esercizio dei poteri datoriali.
Il cambio di manifestazione e di esercizio del potere di controllo sembra, così, necessitare di un aggiornamento che salvaguardi il rinnovato bilanciamento degli interessi.
Da un lato quello dei datori di lavoro di impiegare i dati acquisiti senza trovare ostacoli al soddisfacimento delle proprie prerogative, dall'altro quello dei lavoratori a veder tutelati i propri diritti fondamentali e, in particolare, la dignità e la riservatezza non venendo sottoposti a un controllo che si qualifichi come vessatorio.
Definizione, quest'ultima, che potrebbe non risultare lampante ove la valutazione compiuta a priori sulla legittimità del medesimo si soffermi sui dati "grezzi" e apparentemente "neutri".
La reale intensità del controllo si rinverrà solo con l'elaborazione dei dati che li renda "evidenti" e quindi "comprensibili" nelle loro potenzialità.
La prospettiva di analisi interesserà, quindi, il potere di controllo alla prova delle nuove tecnologie abilitanti e della potenzialità di elaborare dati, soprattutto "non autoevidenti", al fine di comprendere se rientri nella nozione di controllo tracciata dallo Statuto dei lavoratori oppure se l'aggiornamento del potere datoriale necessiti di nuove forme di tutela.
In questo panorama di "supremazia informativa" del datore di lavoro, agevolata dal potenziamento tecnologico, la netta distinzione prevista dall'art. 4 SL tra strumenti di lavoro e di controllo può risultare superata. Conseguentemente, l'autorizzazione all'installazione quale limite al potere datoriale diviene un momento di tutela forse limitato e incapace di soddisfare le nuove esigenze di garanzia.
Contestualmente, affievolendosi la linea di demarcazione tra i poteri datoriali a favore di un nuovo "potere di controllo direttivo" l'indagine deve tenere conto degli ulteriori rischi che possono manifestarsi.

Summary

This study aims to investigate the evolution of employer control power in relation to the modern technologies used in employment relationships.
The research will focus on exercising the power of control in fully digital working contexts and on the protections recognised by workers who operate in these areas for a twofold reason.
Firstly, because the power of control, which has become technological, is strengthened by equipping itself with new abilities that allow access to initially unknown information.
This is not only due to the innovative tools used, but also (and above all) due to the type of data that can be acquired. The latter can be characterised by "non-self-evidence", making them not immediately understandable. Hence, there is a need for a processing phase that makes them intelligible, an operation that places the employer in the position of accessing new information on the workers.
Thanks to digitalisation, the power of control expands in proportion to the information that can be obtained from this "raw data". The cognitive potential of the recent technology, due to its storage and processing capabilities, can thus transform initially "neutral" data into information capable of impacting the condition of workers.
Secondly, because the power of control, enabled with new potential, changes its nature by going beyond the traditional division between employer powers.
Compared to previous technology, the new digital tools do not only intervene when the service is performed but extend the use time. This allows the period of access to information to be varied, anticipating, or postponing it, interfering in the decision-making phase and - consequently – exercising employer powers.
The change in manifestation and exercise of the power of control thus seems to require an update that safeguards the renewed balance of interests.
On the one hand, the employers may use the data acquired without finding obstacles their authority; on the other, the workers may see their fundamental rights protected and, in particular, their dignity and privacy by not being subjected to any control that may represent a vexation.
The latter definition may not be clear if the a priori evaluation of the legitimacy of the same focuses on "raw" and apparently "neutral" data.
The actual intensity of control will only be found with data processing that makes them "evident" and, therefore "understandable" in their potential.
The analysis perspective will therefore concern the power of control, testing the modern enabling technologies and the potential to process data, especially "not self-evident", to understand whether it falls within the notion of control outlined by the Workers' Statute or whether the updating of employer power requires new forms of protection.
In this panorama of the employer's "informational supremacy" facilitated by technological enhancement, the clear distinction provided by art. 4 of Workers' Statute between work and control tools may be outdated. Consequently, the installation authorisation as a limit to employer power becomes a protection, perhaps limited and incapable of satisfying the new guarantee needs.
At the same time, as the line of demarcation between employer powers becomes blurred in favour of a new "managerial control power", the investigation must consider the further risks that may arise.

Sommario

Premessa

Il presente studio si propone di indagare l'evoluzione del potere di controllo datoriale in relazione alle nuove tecnologie impiegate nei rapporti di lavoro.
La ricerca si concentrerà sul modo di esercitare il potere di controllo in contesti lavorativi integralmente digitali e sulle tutele riconosciute ai lavoratori che operano in tali ambiti per una duplice ragione.
In primo luogo, perché il potere di controllo, divenuto tecnologico[1], si rafforza dotandosi di nuove abilità che consentono di accedere a informazioni originariamente ignote.
Ciò non solo in ragione degli strumenti innovativi impiegati, ma anche (e soprattutto) per la tipologia di dati acquisibili.
Quest'ultimi, infatti, possono essere caratterizzati da una "non autoevidenza" risultando non immediatamente comprensibili. Da qui la necessità di una fase di elaborazione che li renda intellegibili, operazione che pone il datore di lavoro nella condizione di accedere a nuove informazioni sui lavoratori.
Grazie alla digitalizzazione, dunque, il potere di controllo si dilata in maniera proporzionale alle informazioni che possono essere ottenute da questi "*raw data*"[2].
In secondo luogo, perché il potere di controllo, abilitato a nuove potenzialità, modifica la propria natura travalicando la tradizionale divisione tra poteri datoriali.
I nuovi strumenti digitali, rispetto alla tecnologia precedente, non intervengono solo nel momento di esecuzione della prestazione, ma ampliano il tempo di utilizzo. Ciò consente di variare il periodo di accesso alle informazioni, anticipandolo o posticipandolo, interferendo sulla fase decisionale e – conseguentemente - sull'esercizio dei poteri datoriali.
Le potenzialità cognitive della nuova tecnologia, in ragione delle capacità di archiviazione ed elaborazione, possono mutare dati originariamente "neutri" in informazioni capaci di incidere sulla condizione dei lavoratori.
Acquisire dati grezzi "non autoevidenti" per finalità di controllo ed elaborarli, per comprenderne il valore, pone il datore di lavoro in una condizione di "supremazia informativa" valida non solo a monitorare, ma anche a prendere decisioni.
Ne è di esempio la possibilità di classificare i prestatori sulla base di elementi ignoti *ab origine* acquisiti a seguito dell'interpretazione.
Ciò consente al datore di lavoro non solo di monitorare, ma anche di organizzare l'attività lavorativa.
Il controllo tecnologico diviene, così, la porta preferenziale attraverso cui acquisire informazioni, declinando in forme inedite i tradizionali poteri datoriali.
La *summa divisio* tra potere di controllo e direttivo sembra, con ciò, affievolirsi alla luce delle nuove potenzialità tecnologiche che delineano una ibridazione tra i poteri e dando forma a un nuovo "potere di controllo direttivo"[3].
Il potere di controllo appare, così, non solo rafforzato ma anche più sofisticato sia per la capacità di elaborare dati "non autoevidenti" - da cui trarre nuove informazioni - sia per le potenzialità decisionali rimesse al datore di lavoro.

---

[1] Cfr. Tufo M., *Lo Statuto dei lavoratori alla prova della Quarta Rivoluzione Industriale*, in Mingione E., Scarpelli F., Giasanti L. (a cura di), *Lo Statuto dei lavoratori alla prova dell'oggi: Una rilettura critica da parte degli studiosi di nuova generazione,* Feltrinelli, Milano, 2022*, pp. 39 ss.* Consultabile al *link: https://fondazionefeltrinelli.it/app/uploads/2022/11/Finale_StatutoLavoratori-1.pdf.*

[2] L'impiego di sistemi algoritmici o di IA i cui utenti ignorano i contenuti o gli output di elaborazione (come nel caso dei dati "grezzi") costituisce una peculiarità della società moderna definita come *Black Box Society*. Cfr. Pasquale F., *The Black Box Society: The Secret Algorithms That Control Money and Information,* Harvard*, 2*015.

[3] In merito anche Laura Tebano che giunge a individuare tale potere partendo da un'analisi del potere direttivo. Tebano L., *Lavoro, potere direttivo e trasformazioni organizzative*, Editoriale Scientifica, Napoli, 2020.

L'impiego di strumenti tecnologici porta a modificare profondamente le facoltà rimesse al potere di controllo, consentendo di ampliare lo spettro dei dati posti nella disponibilità del datore di lavoro.
Il controllo muta la propria natura esorbitando dall'ambito della mera sorveglianza e intercettando funzioni afferenti ad altri poteri datoriali.
La digitalizzazione del lavoro amplia, in questo modo, in modo significativo i poteri datoriali[4] rendendo sempre più sfumato il confine tra osservabilità dei lavoratori, controllo delle attività e gestione delle prestazioni in forza delle innovative potenzialità di acquisizione e disvelamento dei dati.
La genesi di tale inedita manifestazione di "potere di controllo direttivo" sembra trovare conferma nel confine definitorio, sempre più labile, tra strumenti di lavoro e strumenti di controllo in cui l'elemento dell'indispensabilità allo svolgimento della prestazione lavorativa si intreccia indissolubilmente a quello di monitoraggio dei dati e possibile elaborazione degli stessi.
La nuova tecnologia abilitante accosta, quindi, sempre più le finalità di impiego dei dispositivi rendendo complessa la distinzione in strumenti di lavoro che incorporano (anche involontariamente) il controllo.
Controllo che si manifesta non solo in un'attività di monitoraggio, bensì anche in elaborazioni interpretative volte a comprendere il significato dei dati acquisiti.

Risulta, quindi, l'utilizzabilità delle informazioni (raccolte o elaborate) l'argine posto a tutela dei lavoratori.
Proprio il potenziale di acquisire nuove informazioni mediante processi di analisi e la spendibilità delle stesse demarca il confine tra le tutele che, in maniera disomogenea, si trovano descritte in distinte discipline: da quella statutaria a quella *privacy*, passando per quelle *jure condendo* dedicate all'Intelligenza Artificiale e al *management* algoritmico.
Mentre rimangono, quindi, invariati i valori sottesi alle tutele dei lavoratori appare, invece, disomogeneo il grado di tutele vigenti a fronte dei mutamenti intercorsi.

Il cambio di manifestazione e di esercizio del potere di controllo sembra, così, necessitare di un aggiornamento che salvaguardi il rinnovato bilanciamento degli interessi.
Da un lato quello dei datori di lavoro di impiegare i dati acquisiti senza trovare ostacoli al soddisfacimento delle proprie prerogative, dall'altro quello dei lavoratori a veder tutelati i propri diritti fondamentali e, in particolare, la dignità e la riservatezza non venendo sottoposti a un controllo che si qualifichi come vessatorio.
Definizione, quest'ultima, che potrebbe non risultare lampante ove la valutazione compiuta a priori sulla legittimità del medesimo si soffermi sui dati "grezzi" e apparentemente "neutri".
La reale intensità del controllo si rinverrà solo con l'elaborazione dei dati che li renda "evidenti" e quindi "comprensibili" nelle loro potenzialità.

Si delinea, perciò, una sorta di "cortocircuito" nelle tutele: per poter comprendere se il controllo sia legittimo o vessatorio, il datore di lavoro deve necessariamente elaborarli e, quindi, utilizzarli.
Per fare ciò dovrà, però, compiere una valutazione preventiva sulla legittimità del controllo, il cui valore sarà effimero data la parzialità del risultato a cui è giunto analizzando dati "non autoevidenti".

[4]Cfr. Aloisi A., *Regulating Algorithmic Management at Work in the European Union: Data Protection, Non-Discrimination and Collective Rights*, 2022, p. 4, consultabile su:
https://www.researchgate.net/publication/364178531_Regulating_Algorithmic_Management_at_Work_in_the_European_Union_Data_Protection_Non-Discrimination_and_Collective_Rights; Loi P., *Il rischio proporzionato nella proposta di regolamento sull'IA e i suoi effetti nel rapporto di lavoro,* in *Federalismi.it*, Focus lavoro, persona, tecnologia n. 4 del 8 febbraio 2023, p. 240.

Parimenti, anche la valutazione sui rischi connessi all'impiego dei dati, potrebbe risultare insoddisfacente ove il valore degli stessi risulti sconosciuto al momento dell'analisi.

La prospettiva di analisi interesserà, quindi, il potere di controllo alla prova delle nuove tecnologie abilitanti e della potenzialità di elaborare dati, soprattutto "non autoevidenti", al fine di comprendere se rientri nella nozione di controllo tracciata dallo Statuto dei lavoratori oppure se l'aggiornamento del potere datoriale necessiti di nuove forme di tutela.
In questo panorama di "supremazia informativa" del datore di lavoro, agevolata dal potenziamento tecnologico, la netta distinzione prevista dall'art. 4 SL tra strumenti di lavoro e di controllo può risultare superata. Conseguentemente, l'autorizzazione all'installazione quale limite al potere datoriale diviene un momento di tutela forse limitato e incapace di soddisfare le nuove esigenze di garanzia.

Contestualmente, affievolendosi la linea di demarcazione tra i poteri datoriali a favore di un nuovo "potere di controllo direttivo" l'indagine deve tenere conto degli ulteriori rischi che possono manifestarsi. Ove, infatti, il potere di controllo si ibridi è necessario considerare le conseguenze che un monitoraggio inferenziale può avere nei riguardi dei prestatori.
La ricerca non potrà, quindi, esimersi da valutare alcune minacce connesse all'esercizio della nuova forma di "potere di controllo direttivo" come quelle inerenti alla possibilità di compiere una profilazione dei lavoratori, di accedere alle loro opinioni o di compiere scelte discriminatorie.
Lo studio delle ulteriori criticità connesse all'elaborazione dei dati verrà circoscritto ad alcuni fenomeni selezionati le cui ricadute possono maggiormente impattare sulle tutele dei lavoratori.

***

Prima di addentrarsi nella prospettiva di analisi sembra opportuno proporre un breve *excursus* diretto a definire il panorama di riferimento e le problematiche che esso solleva.
Lo sviluppo introdotto dall'Industria 4.0[5] ha portato a una radicale trasformazione delle imprese che, grazie a processi di digitalizzazione abilitati dalla tecnologia dell'Informazione e Comunicazione (ICT), ha modificato le modalità di esecuzione del lavoro e la gestione del personale.
Lo spazio e il linguaggio digitale "*stanno prendendo il posto della fabbrica fordista del '900, come ambiente generale delle prestazioni di lavoro*"[6] manifestando una diffusa tendenza all'automazione e alla informatizzazione dell'impresa adducendo, così, un cambiamento nei metodi organizzativi e di controllo[7].

---

[5] Tullini P., *Il controllo a distanza attraverso gli strumenti per rendere la prestazione lavorativa. Tecnologie di controllo e tecnologie di lavoro: una distinzione possibile*, in Tullini P. (a cura di) *Controlli a distanza e tutela dei dati personali*, Giappichelli Editore, Torino, 2017, p. 118 nota 67; Dessì O. *Il controllo a distanza sui lavoratori. Il nuovo art. 4 Stat. lav.*, Edizioni Scientifiche Italiane, Napoli, 2017, pp. 177-181; Seghezzi F., *La nuova grande trasformazione. Lavoro e persona nella quarta rivoluzione industriale*, ADAPT University Press, 2017, p. 150, in cui l'autore sottolinea l'impatto della nuova tecnologia sui sistemi produttivi e organizzativi; Martini D., *Industria 4.0: una prima riflessione critica,* in L'industria, n. 3, 2016, p. 385; Del Punta R., *Un diritto per il lavoro 4.*0, in Cipriani A., Gramolati A., Mari G (a cura di), *Il lavoro 4.0. La IV rivoluzione industriale e le trasformazioni delle attività lavorative*, FUP, Firenze, 2017, pp. 225 ss.; Lombardi M., Macchi M., *Il lavoro tra intelligenza umana e intelligenza artificiale*, in Cipriani A., Gramolati A., Mari G (a cura di), *Il lavoro 4.0. La IV rivoluzione industriale e le trasformazioni delle attività lavorative*, FUP, Firenze, 2017, pp. 225 ss.; Tiraboschi M., Seghezzi F., *Il Piano nazionale Industria 4.0: una lettura lavoristica*, in *Labour&Law Issues (LLI),* vol. 2, n. 2, 2016, pp. 13 ss.; Ingrao A., *Il Controllo distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata*, Cacucci Editore, Bari, 2018, pp. 68 -74; Dagnino E., *Dalla fisica all'algoritmo: una prospettiva di analisi giuslavoristica,* ADAPT University Press, 2019, pp. 39-44; Santucci R., *La quarta rivoluzione industriale e il controllo a distanza dei lavoratori*, in *Il Lavoro nella giurisprudenza*, n. 1, 2021, pp. 19 ss.; Cipriani A., Gramolati A., Mari A. (a cura di), *La Quarta Rivoluzione industriale e le trasformazioni delle attività lavorative*, Firenze University Press, 2018, disponibile *online.*
[6] Treu *T., La digitalizzazione del lavoro: proposte europee e piste di ricerca,* in *Federalismi.It*, n.9, 2022, p. 193 il quale precisa che "*le piattaforme si candidano a diventare i principali strumenti operativi dell'impresa, fino a svolgere in tutto o in parte le funzioni di datori di lavoro".*
[7] Cfr. Ingrao A., *Il Controllo distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata*, Cacucci Editore, Bari, 2018, p. 69.

La prima novità introdotta dalle tecnologie ICT è il venir meno dei parametri che hanno sempre caratterizzato (e misurato) la prestazione lavorativa: il luogo e il tempo.
Grazie alla digitalizzazione, in un numero crescente di casi l'attività lavorativa può essere eseguita "*in ogni luogo, in ogni tempo e con ogni dispositivo*"[8].
Le prestazioni divengono, in tal modo, "multilocali" o "multispaziali"[9] potendo essere adempiute non solo in presenza, all'interno dei luoghi di lavoro, ma anche a distanza grazie al supporto dei nuovi strumenti informatici.
Anche quando, però, l'attività lavorativa viene svolta in un luogo di lavoro "tradizionale", ovvero "fisico", questa può "traslare" in un ambiente "virtuale", in cui può essere ricreato l'intero *habitat* aziendale.
In secondo luogo, le tecnologie introdotte dall'Industria 4.0 amplificano le potenzialità di acquisire, elaborare e condividere dati.
Le tecnologie abilitanti poste a servizio dei lavoratori rendono possibile l'esecuzione di prestazioni "native digitali" in ambienti virtuali, al contempo datificandole. La digitalizzazione sviluppa, infatti, il contestuale fenomeno della datificazione[10] dei rapporti di lavoro, convertendo in dati le attività compiute in ambienti virtuali.
Il lavoro può, quindi, essere osservato mediante nuovi *output* che codificano l'azione, ovvero i dati provenienti dai "*virtual office*"[11].
Il lavoro si organizza in nuove architetture improntandosi sulle caratteristiche degli strumenti digitali dotati di capacità di archiviazione ed elaborazione dei dati. Ciò determina un incremento del potere di controllo in ragione sia della commistione tra strumento di lavoro e di monitoraggio sia delle abilità di analisi di cui sono dotati.
Nel processo di innovazione del lavoro vi è, dunque, una costante: l'utilizzo di dati (sempre più spesso "non autoevidenti") e il necessario intervento di una fase intermedia, spesso interamente automatizzata, per poter comprendere il significato delle informazioni.
Tra acquisizione e utilizzo dei dati vi è, quindi, un momento di elaborazione capace di "tradurne" il significato e idoneo a disvelare nuove informazioni prima non comprensibili.
La diffusione delle tecniche di *Data Analysis* influenza, conseguentemente, l'intensità del controllo datoriale, divenuto sempre più sofisticato attraverso una gestione *Data Driven.*

---

[8] L'espressione "*working anytime, anywhere and on any device*" è stata utilizzata per spiegare il fenomeno della remotizzazione del lavoro. Tra i tanti Popma J., *The Janus face of the "New Way of Work' Rise risk and regulation of nomadic work*, ETUI Working Paper, n. 7, 2013.

[9] In merito è stato affermato che "*in tutti i casi in cui l'attività lavorativa "esce" totalmente o parzialmente dagli spazi aziendali, non si svolge più "nell'impresa", il potere direttivo e il potere di controllo risultano sempre più intrecciati e richiedono un ripensamento circa il contenuto e i limiti dei tradizionali poteri del datore di lavoro*". Piccinini I., Isceri M., *IA e datori di lavoro: verso una e-leadership?,* in *Lavoro Diritti Europa*, 1 maggio 2021 consultabile al *link*: https://www.lavorodirittieuropa.it/dottrina/principi-e-fonti/710-ia-e-datori-di-lavoro-verso-una-e-leadership. Cfr. anche Greco L., *Tempo per lo spazio: riflessioni sui "luoghi" di lavoro*, in *Labour & Law Issues (LLI)*, vol. 9., n. 1, 2023, pp. 1 ss.; Angeletti L., *Dignità e libertà della persona che lavora tra luoghi fisici e spazi immateriali*, in Mingione E., Scarpelli F., Giasanti L. (a cura di), *Lo Statuto dei lavoratori alla prova dell'oggi: Una rilettura critica da parte degli studiosi di nuova generazione,* Feltrinelli, Milano, 2022, pp. 29 ss. Consultabile al *link: https://fondazionefeltrinelli.it/app/uploads/2022/11/Finale_StatutoLavoratori-1.pdf.*

[10] La datificazione è il processo tecnologico che trasforma vari aspetti della vita sociale o della vita individuale in dati che vengono successivamente trasformati in informazioni dotate di nuove forme di valore anche economico. Cfr. Vocabolario Treccani https://www.treccani.it/vocabolario/datificazione_%28Neologismi%29/.

[11] A riguardo Dagnino ricostruisce l'evoluzione dei luoghi di lavoro digitali che è iniziata con il c.d. "*home office*" ove il telelavoratore lavora presso un postazione fissa presso il proprio domicilio o altro luogo vicino; per passare alla fase di c.d. "*mobile office*" a seguito della prima diffusione di dispositivi portatili quali *laptop* e telefoni cellulari che consentono di eseguire la prestazione anche il "luoghi terzi" rispetto al domicilio; fino a giungere al c.d. "*virtual office*" realizzabile grazie alle tecnologie *ICT* e in grado di riprodurre un luogo di lavoro digitale incluse le dinamiche relazionali. Dagnino E., *Dalla fisica all'algoritmo: una prospettiva di analisi giuslavoristica,* ADAPT, University press, 2019, p. 28.

Il controllo dei dipendenti si trasforma in "controllo dei dati"[12].

Tale trasformazione del lavoro conduce ad alcune conseguenze.
In primo luogo, la prestazione "digitalizzata" trasforma la modalità di controllo esercitabile sui lavoratori. La possibilità di osservare i prestatori che utilizzano dispositivi informatici per l'esecuzione (integrale) della loro attività, comporta il passaggio da un controllo "in presenza" a un controllo "a distanza" mediante l'ausilio di "*strumenti"* (secondo il lessico utilizzato dall'art. 4 SL *post*-riforma).
In secondo luogo, la digitalizzazione e la datificazione permettono (potenzialmente) di osservare e comprendere ogni aspetto non solo professionale, ma anche personale dei lavoratori digitali.
Tali aspetti non risultano, però, "immediatamente comprensibili", ma lo diventano solo all'esito di un necessario processo interpretativo. Datificare l'attività lavorativa non restituisce, infatti, dati immediatamente "autoevidenti".
A differenza dell'osservazione a distanza di una prestazione "analogica" (compiuta fisicamente sul luogo di lavoro) che restituirà un'immagine, un suono o, comunque, un dato immediatamente interpretabile, l'acquisizione delle "tracce digitali" lasciate dai lavoratori in contesti virtuali non risulta sempre *ictu oculi* significativa.
La fase di elaborazione e interpretazione dei dati diviene, pertanto, un passaggio essenziale per giungere alla comprensione dei medesimi che risultano, altrimenti, "non autoevidenti".

Alla luce di ciò, appare necessario indagare come il controllo delle prestazioni "native digitali" venga esercitato e se la normativa a tutela della dignità e riservatezza dei lavoratori sia in grado di far fronte alle nuove esigenze poste da una tecnologia sempre più abilitata a compiere *"sofisticate operazioni di rielaborazione e confronto per aggregazione dei dati*"[13].

***

Svolte queste premesse è possibile definire il piano d'indagine.
Il capitolo I procede ad una ricostruzione, seppur sintetica, dei dispositivi informatici impiegati nel contesto lavorativo odierno.
L'analisi inerisce necessariamente un approfondimento di tipo interdisciplinare, soprattutto da un punto di vista economico e sociologico[14], al fine di comprendere gli obiettivi che tali discipline si prefiggono di ottenere nei contesti lavorativi mediante le nuove tecnologie, nonché gli strumenti impiegati per raggiungerli[15].

---

[12] Definito anche come *Big Data Analytics* in ragione dell'eterogeneità e dei grandi volumi delle informazioni fornite dai dispositivi digitali impiegati. In merito Rota A., *Rapporto di lavoro e big data analytics: profili critici e risposte possibili*, *Labour & Law Issues (LLI)*, 2017, vol. 3, n. 1, pp. I34 ss; Dagnino, E., *People analytics: lavoro e tutele al tempo del management tramite big data*, *Labour & Law Issues (LLI),* vol. 3, n. 1, pp. R37 ss., Dessì O., *Il Controllo a distanza sui lavoratori. Il nuovo art. 4 Stat. lav*., Edizioni Scientifiche Italiane, Napoli, 2017 pp. 181-185; Stizia A., Lopez B., *Le più avanzate modalità di controllo sul lavoratore: machine learning e social media*, in Pisani C., Proia G., Topo A. (a cura di) *Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro*, Giuffrè Editore, Milano, 2022, pp. 358 ss.
[13] Zanetti P., *Impresa, lavoro e innovazione tecnologica*, Giuffrè Editore, Milano, 1985, pp. 68-70.
[14] Biagi M., Treu T., *Lavoro e Information Technology: riflessioni sul caso italiano*, in *Diritto della Relazioni Industriali (DRI),* n. 1, 2002, p. 5 in cui gli autori riconoscono che i processi di trasformazione dei sistemi produttivi devono essere osservati "*anzitutto come fenomeno sociologico ed economico*".
[15] Il diritto del lavoro è, infatti, un "*diritto necessariamente dinamico avendo alla propria base il contratto di lavoro connesso funzionalmente alle organizzazioni produttive e strutturato in modo che i contenuti del rapporto di lavoro si modifichino in funzione dei mutamenti organizzativi e produttivi*". Così Santucci R., *La quarta rivoluzione industriale e il controllo a distanza dei lavoratori*, in *Il Lavoro nella giurisprudenza*, n. 1, 2021, p. 20.

Una valutazione interdisciplinare arricchisce così la ricerca giuslavoristica di nuove prospettive rispetto alle potenzialità introdotte dall'Industria 4.0 e, in particolare, alla capacità di elaborazione delle informazioni, offrendo un'eccezionale "camera con vista"[16] sulle innovazioni tecnologiche impiegate.
Ed è proprio la capacità di analizzare grandi volumi di dati afferenti ai lavoratori che influenza le prerogative datoriali, specialmente nel modo di controllare i dipendenti.
Al fine di cogliere come si manifesta il controllo tecnologico negli ambienti di lavoro digitali verranno, quindi, esaminati i principali sistemi informativi per la gestione del personale e per l'esecuzione delle prestazioni native digitali.
Questi verranno classificati, secondo una ripartizione proposta dall'autrice, in relazione alla loro funzione, alla tipologia di dati che possono acquisire, nonché ai modelli di analisi attuabili.

Il capitolo II è dedicato al potere di controllo ed è stato suddiviso in due parti. La prima, intitolata "la disciplina del controllo a distanza" analizza l'istituito del controllo a distanza, valutandone *ratio,* l'evoluzione e i problemi ancora irrisolti in relazione al controllo tecnologico.
La seconda parte, dedicata all'utilizzo di sistemi digitali per la gestione del personale e l'esecuzione della prestazione in ambienti virtuali, prende in considerazione la "nuova" fase critica del controllo, rinvenibile nella capacità degli strumenti di lavoro di acquisire ed elaborare dati, articolando tale problematica nelle differenti esigenze normative indicate dalla norma di riferimento, ovvero l'art. 4 SL.
L'obiettivo è indagare se la norma giuslavoristica risulti adeguata a tutelare i lavoratori di fronte alle nuove potenzialità a cui è abilitata la tecnologia, evitando che si verifichi un controllo diretto e vessatorio.
Vengono, pertanto, analizzate da un punto di vista casistico la valutazione della *performance* (in riferimento alle esigenze organizzative e produttive), la valutazione dei rischi da iperconnessione (per la tutela della salute e sicurezza sul lavoro) e, infine, la sicurezza informatica (per la tutela del patrimonio aziendale).

La modifica dell'esercizio del potere di controllo alla luce della digitalizzazione del lavoro delimita l'indagine del III capitolo che analizza le problematicità connesse ad un controllo inferenziale e all'impiego dei dati acquisiti a seguito dell'elaborazione.
In particolare, attraverso un'analisi casistica, vengono affrontate le criticità connesse al trattamento e allo strumento con cui si esegue l'analisi.

Il capitolo IV affronta il tema della tutela dei dati personali dei lavoratori in riferimento ai trattamenti automatizzati. Nel capitolo vengono analizzate le condizioni e i limiti della raccolta e trattamento dei dati personali nell'ambito dei rapporti di lavoro tenendo conto delle criticità connesse all'impiego dei sistemi decisionali o di monitoraggio automatizzati o all'attività di profilazione. L'analisi interessa la normativa *privacy* anche alla luce delle modifiche da ultime introdotte dal Decreto Trasparenza del giugno 2022.

La metamorfosi del potere di controllo e il rinnovato equilibrio tra potere datoriale e tutele riconosciute ai lavoratori porta nel V capitolo a valutare il profondo mutamento di scenario e impone un'analisi critica del quadro normativo a tutela dei diritti dei lavoratori.
La digitalizzazione del lavoro e le nuove potenzialità accordate al potere di controllo pone, infatti, un rinnovamento dello strumentario a tutela dei lavoratori, anche in ragione della commistione dei poteri datoriali ridefiniti nella forma di un ibrido "potere di controllo direttivo".
Il capitolo cercherà, quindi, di proporre alcune soluzioni alle criticità rilevate da un punto di vista *de jure condito* e *de jure condendo*.

[16] Santucci R., *La quarta rivoluzione industriale e il controllo a distanza dei lavoratori*, in *Il Lavoro nella giurisprudenza*, n. 1, 2021, p. 20.

Capitolo 1
Strumenti tecnologici per rendere la prestazione digitale e per la gestione dei lavoratori

Per indagare come il controllo delle prestazioni "native digitali" venga esercitato e se la normativa a tutela della dignità e riservatezza dei lavoratori sia in grado di far fronte alle nuove esigenze poste da una tecnologia sempre più abilitata a compiere *"sofisticate operazioni di rielaborazione e confronto per aggregazione dei dati*"[17] è doveroso procedere ad una ricostruzione, seppur sintetica, dei dispositivi informatici impiegati nel contesto lavorativo odierno.
L'analisi inerisce necessariamente un approfondimento di tipo interdisciplinare, soprattutto da un punto di vista economico e sociologico[18], al fine di comprendere gli obiettivi che tali discipline si prefiggono di ottenere nei contesti lavorativi mediante le nuove tecnologie, nonché gli strumenti impiegati per raggiungerli[19].
Una valutazione interdisciplinare arricchisce così la ricerca giuslavoristica di nuove prospettive rispetto alle potenzialità introdotte dall'Industria 4.0 e, in particolare, alla capacità di elaborazione delle informazioni, offrendo un'eccezionale "camera con vista"[20] sulle innovazioni tecnologiche impiegate.
Ed è proprio la capacità di analizzare grandi volumi di dati afferenti ai lavoratori che influenza le prerogative datoriali, specialmente nel modo di controllare i dipendenti.
Al fine di cogliere come si manifesta il controllo tecnologico negli ambienti di lavoro digitali verranno, quindi, esaminati i principali sistemi informativi per la gestione del personale e per l'esecuzione delle prestazioni native digitali.
Questi verranno classificati, secondo una ripartizione proposta dall'autrice, in relazione alla loro funzione, alla tipologia di dati che possono acquisire, nonché ai modelli di analisi attuabili.

1. Una definizione preliminare di dati "non autoevidenti" e "autoevidenti"
Considerato che il presupposto operativo per il funzionamento dei sistemi informativi che compiono analisi, anche automatizzate, è costituito dalla disponibilità di dati e che questi nel presente studio, sono stati definiti "non autovidenti" e "autoevidenti", si intende fornire una definizione preliminare e una distinzione tra le due tipologie.

Il termine dato "non autoevidente" costituisce una classificazione non normativa e qui impiegata per individuare quei dati non immediatamente comprensibili e per la cui interpretazione è necessaria una fase preliminare di elaborazione/correlazione così che possano restituire un'informazione riferibile a una persona identificata/identificabile.

La categoria dei dati "non autoevidenti" ha quale caratterista comune la non immediata intelligibilità, ossia l'assenza di significato, circostanza che può inibire sia l'identificabilità (di conseguenza anche la corrispondenza univoca) con un soggetto, sia la possibilità di fornire un'informazione allo stesso concernente.

---

[17] Zanetti P., *Impresa, lavoro e innovazione tecnologica*, Giuffrè Editore, Milano, 1985, pp. 68-70.
[18] Biagi M., Treu T., *Lavoro e Information Technology: riflessioni sul caso italiano*, in *Diritto della Relazioni Industriali (DRI),* n. 1, 2002, p. 5 in cui gli autori riconoscono che i processi di trasformazione dei sistemi produttivi devono essere osservati "*anzitutto come fenomeno sociologico ed economico*".
[19] Il diritto del lavoro è, infatti, un "*diritto necessariamente dinamico avendo alla propria base il contratto di lavoro connesso funzionalmente alle organizzazioni produttive e strutturato in modo che i contenuti del rapporto di lavoro si modifichino in funzione dei mutamenti organizzativi e produttivi*". Così Santucci R., *La quarta rivoluzione industriale e il controllo a distanza dei lavoratori*, in *Il Lavoro nella giurisprudenza*, n. 1, 2021, p. 20.
[20] Santucci R., *La quarta rivoluzione industriale e il controllo a distanza dei lavoratori*, in *Il Lavoro nella giurisprudenza*, n. 1, 2021, p. 20.

Possono essere considerati, per esempio, dati "non autoevidenti" gli *exaust data* ossia quei dati di "scarto" che derivano da operazioni informatiche, privi di significato ove raccolti autonomamente perché non rivelatori di alcuna informazione attinente ad una persona fisica o perché non possono ritenersi immediatamente riguardanti la medesima o perché inidonei a identificarla.

Tale condizione può escluderli, in un primo momento, dalla categoria di dati "personali", così come definita dall'art. 4 n. 1 del GDPR che ritiene tali "*qualsiasi informazione riguardante una persona fisica identificata o identificabile*".
La definizione di dato personale risulta, infatti, formata da quattro elementi essenziali*:* l'informazione di qualsiasi natura; il nesso di collegamento tra l'informazione e la persona; l'identificazione/identificabilità della persona; la persona fisica a cui la rappresentazione è collegata.[21].

L'assenza di talune componenti determina, così, una temporanea esclusione dalla categoria di dati personali sino a quando l'interpretazione non ne riveli tutti gli elementi.

Particolarmente complesso può essere, per esempio, definire quando un dato "non autoevidente" sia di fatto "concernente" (ovvero "riguardante") una persona fisica[22] e, quindi, non solo la interessi nel contenuto, ma abbia un impatto su un trattamento che la coinvolga o sui suoi diritti.

La capacità di disvelare tali informazioni solo a seguito dell'elaborazione porta in sè il rischio che un dato considerato originariamente non personale lo divenga dopo il "trattamento" interpretativo.

Ciò può avvenire soprattutto in un contesto lavorativo.
Si deve, infatti, considerare che i lavoratori costituiscono un sistema "chiuso", in quanto tutti i soggetti che lo compongo sono noti e censiti a priori.
Questa "mappatura" favorisce, pertanto, l'identificabilità dei soggetti, in taluni casi anche quando i dati vengono acquisiti in forma aggregata[23].

La qualifica di dato "non autoevidente" non inibisce, dunque, l'acquisizione della caratteristica di dato personale, ove risulti in grado di identificare o rendere identificabile un prestatore una volta analizzato.

---

[21]Gruppo di Lavoro ex articolo 29, parere 4/2007 sul concetto di dati personali pp. 6 ss. Cfr. Ingrao A., *Il controllo a distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata*, Cacucci Editore, Bari, 2018, p. 83 la quale osserva che "*la definizione di dato personale, ben vedere, è formata da quattro componenti essenziali: a) l'informazione; b) la persona fisica a cui la rappresentazione è collegata; c) il rapporto di collegamento tra le informazioni e la persona; d) l'identificazione/identificabilità della persona"*. In merito anche Donini A., Tecniche avanzate di analisi dei dati e protezione dei lavoratori, in Diritto delle Relazioni Industriali (DRI), n. I/XXVIII, 2018, p. 228 ss.

[22] In merito, il Gruppo di Lavoro ex articolo 29 nel Parere 4/2007 sul concetto di dati personali osserva che "*per stabilire se i dati concernono una persona, dovrebbe ricorrere un elemento di contenuto oppure di finalità oppure di risultato*" (p. 10).
Nel primo caso sussiste quando i dati ineriscono una persona; il secondo quando le informazioni saranno probabilmente usate per valutare, trattare o influire sullo stato o sul comportamento di una persona.
Infine, "*un terzo tipo di concernente una persona specifica emerge quando è presente un elemento di risultato. Nonostante l'assenza di elementi di contenuto o di finalità è possibile considerare che i dati concernono una persona quando il loro impiego può avere un impatto sui diritti sugli interessi di quella persona, tenendo conto di tutte le circostanze del caso di specie. Si noti che non è necessario che il risultato potenziale abbia un impatto importante punto è sufficiente che la persona sia trattata in modo diverso rispetto ad altre in seguito al trattamento di tali dati*" (p. 10).

[23] Il Garante per la protezione dei dati personali ha qualificato come "dati personali" quelli utilizzati per valutare i dipendenti, anche resi in forma aggregata. Cfr. *Verifica preliminare: trattamento di dati personali connesso ad un sistema di valutazione dei dipendenti* - 4 novembre 2010. In riferimento alla possibilità di ricondurre anche in maniera univoca dati biometrici ai lavoratori si rinvia a Tebano L., *Poteri datoriali e dati biometrici nel contesto dell'AI Act*, in *Federalismi.it*, n. 25, 2023, pp. 198 ss.

Il peculiare contesto lavorativo sembra, così, potenzialmente favorire l'identificabilità di una persona, anche quando il dato originale sia "non autoevidente".

L'elaborazione di dati "non autoevidenti" può, inoltre, disvelare informazioni non solo personali, ma altresì particolari o biometriche di un lavoratore.
Nel primo caso ove essi siano in grado di rivelare "*l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona*" (art. 9 co. 1 GDPR).
Nel secondo quando i dati personali del prestatore siano "*ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici*"[24].
Quest'ultima ipotesi fa riferimento a quei dati che rivelano caratteristiche fisiche, fisiologiche o comportamentali di un individuo, come può essere la voce[25].
Le peculiarità dei dati biometrici è l'unicità della caratteristica dell'interessato che ne consente l'identificazione univoca e il processo tecnico volto ad estrapolare il dato biometrico a partire dalle caratteristiche del soggetto.
I dati biometrici non costituiscono, dunque, una semplice raccolta dati, ma necessitano di un intervento di analisi.
Così, a titolo esemplificativo, la semplice misurazione della pressione esercitata sui tasti di un *pc* per eseguire una prestazione lavorativa non è di per sé idonea a identificare in modo univoco un soggetto e, pertanto, non può essere considerata "dato biometrico".
Ciò non toglie, però, che in un contesto, come già detto, circoscritto - qual è quello lavorativo - tali dati in ragione del processo tecnico possano consentire o confermare l'identificazione univoca di un prestatore, come nel caso in cui alimentino sistemi algoritmici o di IA predisposti a valutare la *performance* lavorativa[26].
I dati "non autoevidenti", ancorché privi di un significato *ab origine*, hanno così insito un potenziale informativo la cui natura e rilevanza può apparire *prima facie* oscura.

Altra terminologia impiegata nel presente studio è quella di dati "autoevidenti".
Anche in questo caso la categoria non deriva da una classificazione normativa, ma è stata introdotta per identificare tutti quei dati che restituiscono un'informazione in maniera immediata, senza la necessità di un processo di analisi o di correlazione preliminare.

---

[24] Art. 4, n. 14 GDPR. Definizione conforme a quella elaborata dal Gruppo di lavoro ex Articolo 29 per la protezione dei dati Parere 3/2012 sugli sviluppi nelle tecnologie biometriche, adottato il 27 aprile 2012 ("proprietà biologiche, aspetti comportamentali, caratteristiche fisiologiche, tratti biologici o azioni ripetibili laddove tali caratteristiche o azioni sono tanto proprie di un certo individuo quanto misurabili, anche se i metodi usati nella pratica per misurarli tecnicamente comportano un certo grado di probabilità"). Chiarimento ripreso anche dal Garante per la protezione dei dati personali nelle Linee Guida in materia di riconoscimento biometrico e firma grafometrica, di cui all'allegato A del Provvedimento generale prescrittivo in tema di biometria, adottato il 12 novembre 2014.
[25] Cfr. Gruppo di Lavoro ex Articolo 29 per la protezione dei dati, Parere 4/2007 *sul concetto di dati personali*, adottato il 20 giugno 2007, e Parere 3/2012 sugli sviluppi nelle tecnologie biometriche, adottato il 27 aprile 2012.
[26] Tra i dati non strettamente biometrici, ma idonei a identificare in modo univoco un soggetto vengono citati dalla dottrina anche tremolio, intonazione, accento, volume della voce. Per tale ragione l'ultima versione della proposta di Regolamento sui IA ha previsto l'introduzione di una nuova categoria di dati basati sulla biometria che si affianca alla categoria di "dati biometrici" come definiti dal GDPR. In merito Tebano L., *Poteri datoriali e dati biometrici nel contesto dell'AI Act*, in *Federalismi.it*, n. 25, 2023, p. 205, 206.

Nel contesto lavorativo si possono qualificare come dati "autoevidenti", per esempio, le immagini che possono essere acquisite mediante una videocamera di sorveglianza o con uno *screenshot* dello schermo di un *pc*.
In questo caso, infatti, le immagini (che costituiscono i dati acquisiti) restituiscono un'immediata informazione sul lavoratore e su quello che sta svolgendo in un ambiente lavorativo o sul proprio terminale, risultando intellegibili all'osservatore senza necessità di alcun intervento.
Costituiscono, quindi, sicuramente dati "autoevidenti" tutti quelli di natura personale[27] sia in senso oggettivo (come gli elementi caratteristici dell'identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale di un soggetto) sia soggettivo (come opinioni o valutazioni)[28].
In ambito lavorativo rappresentano, così, dati "autoevidenti" la velocità di esecuzione di una prestazione o le pause compiute dal lavoratore in quanto dati personali di natura soggettiva capaci influenzare il datore di lavoro nella propria valutazione "*sul rendimento, sulla produttività, sulla performance del lavoratore*"[29]

Non solo i dati personali, però, sono qualificabili come "autoevidenti".
Sono altresì dati "autoevidenti" quelli di natura "non personale", ovvero non riconducibili a una "persona fisica".
Questo può essere, per esempio, il caso di informazioni afferenti ad una persona giuridica.
Ove, infatti, l'informazione non possa essere considerata come "concernente" una persona fisica, viene meno la natura personale del dato acquisito, ma la sua intellegibilità.

Mentre è possibile affermare, quindi, che tutti i dati personali sono dati "autoevidenti", non è sempre vero il viceversa, dato che possono essere ricompresi tra i dati "autoevidenti" anche quelli di natura non personale.

Un dato "autoevidente" è, quindi, un dato che contiene un'informazione e tale informazione risulta comprensibile senza necessità di un trattamento che ne disveli il significato.

Elemento comune ai dati "autoevidenti" è, quindi, l'intellegibilità e la loro comprensione sin dal momento in cui vengono acquisiti.

2. Funzione degli applicativi

Riprendendo la catalogazione proposta, in riferimento alla funzione degli applicativi questi possono essere distinti in: programmi adibiti a gestire il personale, sistemi utilizzati per fornire spazi virtuali di collaborazione, *software* destinati ad amministrare i clienti (da cui possono essere tratte informazioni indirette sui lavoratori) e a selezionare i candidati.
In ragione delle funzioni individuate, questi possono essere differenziati in:

- sistemi HRIS *(Human Resources Information System)* usati per gestire il personale;
- *software* denominati *Digital workplace* utilizzati per fornire spazi virtuali di collaborazione;
- sistemi CRM (*Customer Relationship Management*) impiegati per amministrare i clienti e da cui possono essere tratte informazioni indirette sull'operato dei lavoratori;

[27] ai sensi dell'art. 4 n. 1 del GDPR.
[28] Cfr. Gruppo di Lavoro ex Articolo 29 per la protezione dei dati, Parere 4/2007 *sul concetto di dati personali*, p. 6.
[29] Ingrao A., *Il controllo a distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata*, Cacucci Editore, Bari, 2018, p. 84 che richiama quanto detto dal Gruppo di Lavoro ex Articolo 29 per la protezione dei dati nella Raccomandazione n. 1/2001 *concernentei dati relativi alla valutazione del personale*, adottato il 22 marzo 2001, WP42.

- sistemi ATS (*Applicant Tracking System*) per la ricerca e selezione del personale.

Si procederà ad una sintetica analisi dei differenti applicativi al fine di comprenderne l'operatività.

2.1. HRIS *(Human Resources Information System)*

I dati utilizzati per la gestione dei lavoratori sono normalmente estratti dal sistema informativo dedicato alle risorse umane denominato *Human Resources Information System* o HRIS[30] e integrati con i risultati di sondaggi o questionari rivoti ai dipendenti[31].
HRIS è definito come un sistema utilizzato per acquisire, conservare e analizzare informazioni riguardanti le risorse umane di un'organizzazione.
Originariamente, i sistemi HRIS erano distinti da altri applicativi utilizzati dell'impresa e destinati a seguire esclusivamente i processi inerenti alle risorse umane.
Con l'avvento della digitalizzazione, i sistemi di HRIS si sono ampliati e integrati con altri *software* in uso presso le aziende, consentendo di gestire un maggior numero di funzioni relative al personale e di offrire applicazioni più sofisticate per le operazioni manageriali e decisionali (per esempio in riferimento al *reporting*).
Oggigiorno, i sistemi di HRIS si integrano con le *suite software* ERP (*Enterprise Resource Planning*)[32], un applicativo utilizzato per gestire le attività quotidiane dalle imprese in riferimento al *business*, alla contabilità, al *project management* e al *performance management*.
Una *suite* ERP aiuta a pianificare, quantificare, prevedere e comunicare i risultati finanziari di un'organizzazione combinandoli con i dati delle risorse umane.
I sistemi HRIS diventano, così, sempre più abilitati al *web* e basati su un'architettura *Internet*. Ciò consente di centralizzare tutti i dati del personale, rendendo possibile accedervi in qualsiasi momento/luogo tramite un *browser web*.
Con la digitalizzazione avviene anche un aumento di attenzione ai sistemi di supporto alle decisioni e di *Business Intelligence* (BI)[33] che vengono ulteriormente implementati all'interno dei sistemi di HRIS, consentendo maggiori capacità di analisi.
Un HRIS è, quindi, un Sistema Informativo delle Risorse Umane composto da diversi componenti *software* (detti moduli) che automatizzano le attività specifiche di ogni processo di gestione di lavoratori come la gestione del lavoro e degli orari, i salari e le retribuzioni, la valutazione delle prestazioni, la mappatura delle competenze ("*soft skill*")[34], la formazione reclutamento e molto altro.

La diffusione di HRIS determina la creazione di grandi quantità di dati sui lavoratori organizzati in *database*.

---

[30] Esempi di HRIS sono il *software* Ecosagile; Cornerstone; Monday.com; Workday; Fluida.
[31] Angrave D., Charlwood A., Kirkpatrick I., Lawrence M., Stuart M., *HR and Analytics: Why HR Is Set to Fail the Big Data Challenge,* in Human Resource Management Journal, vol. 26, no. 1, 2016, pp. 1–11.
[32] Un ERP è un sistema completo che integra tutte le funzioni essenziali per la gestione di un'azienda (Contabilità, Inventario e Gestione degli ordini, Risorse Umane, Gestione delle relazioni con i clienti, Produzione, Catena di fornitura, Servizi, Approvvigionamento, etc.) e che è in grado di automatizzare ed informatizzare i processi e le informazioni dell'intera organizzazione. Per un esempio di software ERP è si veda in www.fluentis.com.
[33] La *Business Intelligence* combina *business analytics*, *data mining*, visualizzazione dei dati, strumenti e infrastrutture per i dati, nonché le *best practice* per permettere alle organizzazioni di prendere più decisioni basate sui dati (si veda in www.tableau.com).
[34] Cfr. Brollo M., *Disciplina delle mansioni (art. 3)*, in Carinci F. (a cura di), *Commento al D. Lgs. 15 giugno 2015, n. 81: le tipologie contrattuali e lo jus variandi,* ADAPT University Press, ADAPT Labour Studies e-Book series, 2015, n. 48, pp. 29-34; Caruso B., *Strategie di flessibilità funzionale e di tutela dopo il Jobs Act: fordismo, post fordismo e industria 4.0,* in *Giornale di Diritto del Lavoro e Relazioni Industriali (DLRI),* n. 1, 2018, pp. 81 ss; Benadusi L., Molina S., *Le competenze. Una mappa per orientarsi*, Fondazione Agnelli, Il Mulino, Bologna, 2018.

Tali dati possono essere centralizzati per elaborare un monitoraggio degli obiettivi raggiunti, per ottenere un reclutamento più efficace ed elaborare previsioni sullo sviluppo di carriera dei lavoratori.

2.2. *Digital Workplace*

Per *Digital Workplace*[35] si intendono quei *software* "collaborativi" che costituiscono dei veri e propri "spazi di lavoro digitale" all'interno dei quali viene svolta non solo la prestazione lavorativa, ma si sviluppano anche le dinamiche relazionali tra lavoratori e tra questi e l'organizzazione.
Un ambiente di lavoro digitale è una forma virtuale del tradizionale ambiente d'ufficio fisico, in cui molti elementi di collaborazione e produttività vengono eseguiti attraverso una combinazione di applicazioni digitali, *cloud computing* e connettività alla rete.
Il termine fa, dunque, riferimento all'ampio ecosistema delle tecnologie sul posto di lavoro.
L'ambiente di lavoro digitale rappresenta una piattaforma interattiva di connessione che raccoglie tutti gli strumenti necessari ai lavoratori digitali per svolgere la prestazione e per sviluppare gli obiettivavi dell'organizzazione.
Una *Digital Workplace* include molteplici applicativi e strumenti collaborativi quali *app* di comunicazione e messaggistica, programmi di archiviazione *cloud*, piattaforme *intranet* aziendali, sistemi di gestione contenuti e condivisione documenti.
La *Digital Workplace* crea, così, un *hub*[36] centralizzato (ovvero una rete informatica) in cui i lavoratori possono accedere alle informazioni e svolgere le proprie attività lavorative, indipendentemente dalla loro ubicazione o dal dispositivo utilizzato.

I più recenti spazi di lavoro digitali[37] sono integrati con ulteriori funzionalità.
I lavoratori, accedendo con il proprio *ID* personale alla *Digital Workplace*, possono connettersi all'azienda, trovando comunicazioni interne e risorse aziendali, ma anche ai colleghi, partecipando alle "*community*" composte da gruppi di lavoro.
La *Digital Workplace* consente di impostare una relazione integrata e condivisa dall'azienda creando automaticamente dei "*topics*", ovvero delle schede di argomenti all'interno di conversazioni o documenti condivisi sulla piattaforma.
Selezionando la scheda desiderata è possibile, in tal modo, accedere a tutti i documenti correlati all'argomento, alle conversazioni inerenti, ai video pertinenti e alle persone coinvolte.
La *Digital Workplace* è anche in grado di offrire ai dipendenti (a secondo del ruolo e della funzione ricoperta) approfondimenti e formazione personalizzata, resi maggiormente accessibili in ragione del flusso di lavoro di ogni soggetto. Questa funzionalità aggrega tutte le risorse di apprendimento disponibili per un'azienda in un unico luogo. Dai corsi di formazione tradizionali ai contenuti di micro-apprendimento, gli utenti possono scoprire, condividere, assegnare e monitorare una grande varietà di *training* come parte naturale della giornata lavorativa.
Viene, così, implementata la formazione *E-learning* e *blended learning*[38] (che consiste in uno studio misto sincrono e asincrono) volta a creare un percorso di approfondimento personalizzato e, altresì, capace di monitorare l'efficacia delle nozioni apprese da ogni soggetto.

---

35 Esempi di *digital workplaces* sono Microsoft 365, Google Suite, Microsoft Viva.
36 Intendendo per *hub* un dispositivo per connettere più elaboratori a una rete e più reti fra loro. Su "dizionari del Corriere" visionabile su https://dizionari.corriere.it/dizionario_italiano/H/hub.shtml.
37 Come Microsoft Viva.
38 Per *blended learning* si intende un approccio formativo che unisce elementi della formazione tradizionale in presenza con attività *online* guidate da un formatore. A differenza dell'E-*learning*, le lezioni *online* non sostituiscono completamente quelle "analogiche". La tecnologia viene, quindi, impiegata per arricchire l'esperienza formativa. Cfr. Tietz Cazeri G., De Santa-

Le potenzialità della piattaforma digitale sono orientate anche a favorire la salute dei lavoratori, aiutando a bilanciare occupazione e tempi di riposo. La *Digital Workplace* può, per esempio, pianificare in maniera specifica gli intervalli di lavoro idonei per ottimizzare concentrazione, apprendimento e benessere dei singoli.
La piattaforma può anche intervenire per fornire suggerimenti "relazionali" personalizzati proponendo strategie per rafforzare i rapporti con i propri colleghi.
Il sistema è, inoltre, abilitato a supportare i *manager* nell'organizzare l'attività lavorativa, rilevando i *trend* (di singoli o gruppi di lavoratori) così da migliorare il bilanciamento tra produttività e il benessere.

La struttura è, dunque, programmata per acquisire e analizzare dati dei lavoratori, mediante sistemi algoritmici o di Intelligence Artificiale (IA), posti a supporto delle differenti funzionalità.

2.3. CRM (*Customer Relationship Management*)

Il concetto di *Customer Relationship Management* (*CRM*) è legato alla gestione delle relazioni con i clienti di un'impresa.
Il *CRM* è una tecnologia basata su *cloud* impiegata per registrare, analizzare e creare *report* delle connessioni attuate dall'azienda con i clienti al fine di migliorare il servizio offerto e "fidelizzare" gli utenti.
Il *software CRM* è in grado di registrare informazioni di contatto sui clienti (come indirizzo *e-mail,* numero di telefono, profilo sui *social media* e altro), indicazioni sulle preferenze di erogazione del servizio, *feedback* sulle prestazioni ricevute e sul grado di soddisfazione[39].
Nel caso, per esempio, di un *CRM* definito "collaborativo", questo monitora la gestione dei contatti con i clienti mediante gli strumenti di comunicazione aziendali (quali telefono o *e-mail*). Il sistema è, così, in grado si riportare anche il *feedback* sulle attività svolte dai dipendenti per raggiungere tale scopo.
Dai *CRM* è, quindi, possibile trarre informazioni in relazione all'obiettivo o al risultato conseguito dai lavoratori, intesi come *outcome* dell'attività (concepito, per esempio, quale ammontare di fatturato conseguito in una determinata zona geografica) oppure come *output* (rappresentato dalla quantità di attività svolta dal dipendente come può essere il numero di contatti intrattenuto con i clienti).
Tali sistemi sono, dunque, in grado di fornire *report* "indiretti" (ma precisi) sull'attività lavorativa compita dai singoli dipendenti in relazione alle operazioni svolte con i clienti.

2.4. ATS (*Applicant Tracking System*)

Negli ultimi anni le aziende, soprattutto di grandi dimensioni, hanno iniziato a utilizzare *software,* noti come ATS *(Applicant Tracking System),* a supporto dei processi di ricerca e selezione del personale.
Gli ATS vengono utilizzati per raccogliere e classificare i *curricula* che le aziende ricevono, consentendo di monitorare in maniera centralizzata l'intero processo di selezione e reclutamento (dalla pubblicazione dell'annuncio di ricerca, al processo di valutazione e assunzione).

Eulalia L. A., Pavan Serafim M., Anholon R., *Training for Industry 4.0: a systematic literature review and directions for future research,* in *Brazilian Journal of Operations & Production Management*, vol. 19, n. 3, 2022, pp. 1-19.

[39] Una tecnologia analoga è stata oggetto del giudicato della Corte di Cass. del 9 febbraio 2016, n. 2531 che ha analizzato la legittima installazione di "*un sistema informatico di rilevazione automatica delle operazioni di sportelleria (che) era costituito dalla trasmissione in via informatica su un server locale (…) di tutti i dati relativi alle varie operazioni con i clienti, destinate a essere trascritte/stampate su un giornale di fondo, la trasmissione riguardava i dati relativi alla natura dell'operazione, al cliente, all'operato dello sportello ed era finalizzata alla gestione della contabilità giornaliera, che a sua volta consentiva, in caso di errore, di individuare l'operatore che lo aveva effettuato (…).*". La Suprema Corte in tal caso ha ravvisato la violazione dell'art. 4 comma 2 SL (vecchio testo) per assenza di accordo sindacale in quanto, anche se il dispositivo rispondeva ad esigenze organizzative-produttive, comportava un controllo dei lavoratori. Cfr. Gragnoli E., *Gli strumenti di controllo e mezzi di produzione*, in *Variazioni su Temi di Diritto del Lavoro*, n. 4, 2016, p. 661; Ingrao A., *Il controllo a distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata,* Cacucci Editore, Bari, 2018, pp. 175-176.

Dato il volume dei CV che le aziende ricevono quotidianamente, gli ATS sono supportati da sistemi di Intelligence Artificiale (IA) per l'esecuzione delle differenti fasi del processo di selezione.
In un primo momento le offerte di lavoro vengono promosse su *Internet* mediante *software* come *Google Ads* o i *social media*. Successivamente, viene effettuata una prima selezione dei CV ricevuti mediante lettura del testo automatica per la ricerca delle parole chiave codificate come rilevanti per l'organizzazione.
Questi sistemi possono integrare anche un processo di valutazione dei candidati, includendo un colloquio virtuale supportato da IA. In questo caso, i soggetti vengono intervistati utilizzando *chatbot*[40] per acquisire informazioni e scremare ulteriormente l'elenco dei candidati.
Le interviste possono essere oggetto di ulteriore analisi mediante programmi[41] in grado di analizzare il discorso e le espressioni facciali.
I risultati dell'analisi di un sistema AST mirano a riscostruire informazioni non solo sulle abilità professionali del candidato, ma anche sulle capacità collaborative, sulla personalità e sulle attitudini cognitive generali e trasversali possedute.
I sistemi ATS si propongono, quindi, di elaborare e correlare un gran numero di dati sui candidati.

3. Categorie di dati acquisiti

La digitalizzazione dei processi di gestione dei lavoratori genera grandi quantità di dati che portano a creare dei *dataset*[42].
La creazione di queste "banche dati" costituisce il nuovo valore per le imprese tanto che è stato osservato che *"(…) i dataset più rilevanti per un'impresa sono quelli che l'impresa crea per sé stessa in quanto conosce il contesto nel quale sono stati creati e le finalità per la quale erano creati. Le principali innovazioni possono derivare proprio dai dataset costruiti da un'impresa per un uso interno, non destinati fin dall'inizio a terzi o al mercato*"[43].

I *dataset* aziendali contengono dati molto eterogenei tra loro che, secondo una classificazione proposta dall'autrice, possono essere ordinati nelle seguenti categorie:
a) per provenienza: i dati possono essere interni o esterni all'organizzazione, nonché interni o esterni alla Direzione delle Risorse Umane.

b) Per tipologia[44]: in questo caso, i dati possono essere strutturati (ovvero provenienti dal *dataset*), semistrutturati o non strutturati (come quelli ottenibili dai *social network* come immagini, video e *file* di testo).

[40] Tra i *chatbot* più conosciuti ci sono vi sono *Mya, Olivia, Myra* e *Yva*. I dettagli di ogni *chatbot* sono consultabili sulle pagine dei suoi produttori: rentalmya.com, www.olivia.ai, www.myralabs.com, yva.ai.
[41] Come quelli utilizzati dalla società HireVue. Secondo l'azienda, ogni minuto di video li fornisce più di un milione di dati che vengono analizzati dai sistemi di *apprendimento automatico* per essere rilevati tratti come l'intelligenza emotiva e le abilità sociali. Inoltre, i sistemi HireVue esaminano i risultati dei test cognitivi e neurologici effettuati dai candidati somministrati sotto forma di *gaming*. www.hirevue.com.
[42] Secondo la definizione fornita da Treccani, un *dataset* in informatica è "*un insieme di dati organizzati in forma relazionale. Ha una struttura tabellare, dove di solito ogni colonna rappresenta una variabile e ogni riga corrisponde a una osservazione. È usato anche in statistica*". Consultabile *online* su https://www.treccani.it/enciclopedia/data-set_%28Dizionario-di-Economia-e-Finanza%29/#:~:text=data%20set%20In%20informatica%2C%20insieme,%C3%88%20usato%20anche%20in%20statistica.
[43] Audizione Microsoft, 9 ottobre 2018. Analoghe considerazioni sono state svolte anche da IBM il 22 ottobre 2018.
[44] Secondo la ricerca presentata il 13 ottobre 2016 dall'Osservatorio HR Innovation Practice del Politecnico di Milano, *HR Analytics & Big Data Driven Innovation: cosa significa e come impostare una roadmap di innovazione*, in collaborazione con Cornerstone. Disponibile *online*.

Per dati strutturati si intende quella tipologia di dati che possono essere organizzati mediante sistemi tradizionali quali *Excel*, SPSS, SAS o con *software* di *database*[45] relazionali.
I dati strutturati sono, dunque, quelli creati utilizzando uno schema predefinito e organizzati in un formato tabellare ove, ad ogni casella, corrisponde un valore specifico.
I dati strutturati possono essere raggruppati secondo categorie e organizzati mediante righe e colonne che "vincolano" i dati a specifici valori che li rendono coerenti e calcolabili.
I dati strutturati derivano, generalmente, da sistemi *HRIS*, ma possono pervenire anche da fonti esterne.
Normalmente costituiscono dati strutturati:

- dati identificativi: quali *ID* dipendente, data di registrazione alla piattaforma, città e paese di provenienza;
- dati personali: come età, sesso, etnia;
- dati inerenti all'attività lavorativa come:
    - posizione lavorativa: dipartimento di appartenenza, funzione organizzativa, *business unit*, tipo di mansione/titolo, ore lavorate, retribuzione/retribuzione;
    - prestazioni lavorative: valutazioni delle prestazioni lavorative (complessive e a livello di competenza);
    - informazioni sulle assunzioni/storia del rapporto di lavoro: data di assunzione originaria, data di cessazione (se cessata), anzianità di servizio, motivo di cessazione, tipo di cessazione (volontaria o involontaria), mobilità interna, formazione.
- dati relativi a sondaggi e questionari;
- dati di posizione: come quelli ricavabili da un sistema GPS;
- dati M2M (*Machine to Machine*) generati da sensori (quali RFID[46], *Bluetooth*, NFC, WiFi, etc.).

I dati semistrutturati sono dati che possono essere anch'essi organizzarti per categorie, ma mediante tecniche di analisi più complesse.
I dati semistrutturati sono, quindi, caratterizzati dall'assenza di una struttura rigida e formale, anche se contengono elementi di *tag* o altri tipi di *markup* (ovvero "elementi evidenziati") che consentono di raggrupparli.
Per esempio, viene considerato un dato semistrutturato una classificazione di *e-mail* compiuta in riferimento al mittente o al destinatario della missiva.
La categoria dei dati seminstrutturati include:

- dati dei *social media* (ad es. messaggi di *Facebook* o *Twitter*);
- dati del telefono cellulare;
- dati da *e-mail*;
- dati biometrici;
- dati di navigazione.

Infine, tutti i dati che non si adattano ad uno schema classificatorio e che non possono essere organizzati in categorie sono definiti dati non strutturati.

---

[45] Secondo la definizione fornita da Treccani, un *database* è un "*archivio elettronico di dati correlati, registrati nella memoria di un computer e organizzati in modo da poter essere facilmente, rapidamente e selettivamente rintracciabili uno per uno, oppure per gruppi determinati, mediante appositi programmi di gestione e di ricerca*". Consultabile *online* su https://www.treccani.it/vocabolario/data-base/#:~:text=%E2%80%93%20Archivio%20elettronico%20di%20dati%20correlati,data%20base%2C%20ma%20pi%C3%B9%20propr.

[46] Tale tecnologia era, per esempio, implementata nei braccialetti elettronici adottati dalla società di igiene urbana AVR di Livorno. Mediante la tecnologia *RFID* l'azienda poteva verificare che gli operatori ecologici avessero correttamente svuotato i cassonetti della spazzatura. In merito Di Meo R., *Tecnologie e poteri datoriali: commento a margine del c.d. braccialetto Amazon*, in *Labour & Law Issues (LLI)*, vol. 4, n. 1, 2018, R5; Ingrao A., *Il Controllo a distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata*, Cacucci Editore, Bari, 2018, p. 189.

Esempi di dati non strutturati sono le informazioni di testo completo (ad es. PDF, documenti *Word*), *file* audio, immagini e video.
Tutti i dati qui elencati costituiscono "dati personali", ai sensi dell'art. 4 del Regolamento 2016/679 (GDPR), in quanti riferibili ad un soggetto identificato o identificabile.

c) Per forma: in questo caso i dati possono essere quantitativi o qualitativi.
I dati quantitativi sono quelli misurabili e illustrabili attraverso i numeri.
Esempi di dati quantitativi sono il numero di dipendenti presenti in azienda, i tassi di remunerazione, la produttività.
I dati qualitativi costituiscono, invece, valutazioni soggettive che rappresentano il punto di vista di un individuo. Di conseguenza, non possono essere soggetti a misurazione.
Costituiscono esempi di dati qualitativi i *feedback* sui sondaggi di opinione dei dipendenti o dei clienti (nel caso dei sintemi CRM), valutazioni e revisioni delle prestazioni, risultati di apprendimento e sviluppo.

d) Per scopo: in questo caso i dati possono essere distinti in "dati principali", *exhaust data*[47] (o "dati di scarico" o "metadati"[48]).
I dati principali sono dati generati o registrati per un motivo, un'intenzione o un sistema specifico.
I "dati di scarico" sono dati residui da transazioni digitali, per i quali non esiste uno scopo preliminare e specifico alla loro raccolta avendo un valore e una finalità di trattamento in origine sconosciuti.
Gli *exhaust data* sono dati la cui acquisizione non appare, quindi, fondamentale e vengono assimilati (intenzionalmente o meno) come sottoprodotto di un evento/operazione informatica.
Sono esempi di "metadati":

- il percorso di *clic* su una pagina *web*: consiste nel monitoraggio del comportamento di un utente nel visualizzare una pagina *web* (per esempio: quando e quanto fa *clic* su una pagina, tempo trascorso su una pagina);
- i dati di traffico di *e-mail*/calendario: forniscono informazioni sul comportamento dei soggetti posti in relazione (per esempio: mittente-destinatario, reparto di appartenenza, numero riunioni svolte, argomenti e *timing* delle riunioni).

***

Quanto i dati acquisiti mediante i dispositivi digitali di gestione del personale o per l'esecuzione virtuale della prestazione raggiungono volumi ingenti, vengono definiti "*Big Data*" la cui nozione afferisce a "*the practice of combining huge volumes of diversely sourced information and analysing them, using more sophisticated algorithms to inform decision*"[49].

---

47 Oleary D., Storey V. C., *Discovering and Transforming Exhaust Data to Realize Managerial Value*, in Communications of the Association for Information Systems, vol. 47, paper 15, pp. 315-337; Banno R., Takeuchi S. et all, *Designing overlay networks for handling exhaust data in a distributed topic-based pub/sub architecture, in Journal of Information Processing*, vol. 23, n. 2 pp. 105 – 116.
48 In telematica (ovvero l'insieme delle infrastrutture di reti di comunicazione elettronica per la circolazione di segnali/impulsi tra sistemi informatici interconnessi che veicolano dati di carattere multimediale, nonché queste medesime comunicazioni), i "metadati" sono informazioni che accompagnano i dati di transito definendone e individuando "*le coordinate fondamentali: data e ora del "passaggio", indicazioni quali-quantitative (più o meno specifiche) su provenienza, destinazione, "peso" e velocità, tipologia, natura, formato, se aperto o chiuso/proprietario, e contenuto: tutti oggetto di possibile aggregazione/disaggregazione, elaborazione e, di conseguenza, controllo. Si tratta di masse di dati che circolano in rete (cd. big data) suscettibili di utilizzo a fini commerciali (data mining e data analysis), di controllo politico e anche di difesa dell'ordine pubblico*". In merito Sigismondi I., *Telematica*, voce in Diritto Costituzionale, Treccani consultabile sul sito https://www.treccani.it/enciclopedia/telematica-dir-cost_%28Diritto-on-line%29/.
49 EDPS Opinion 7/2015 *Meeting the challenges of Big Data – A call for transparency, user control, data protection by design and accountability* del 19.11.2015 https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf.

Con il concetto di *Big Data* ci si riferisce, così, alla raccolta, analisi e accumulo ricorrente di ingenti quantità di dati (anche personali) provenienti da fonti eterogenee e oggetto di un trattamento automatizzato mediante tecniche avanzate di analisi al fine di individuare correlazioni, tendenze e modelli[50].
Il concetto di *Big Data* si articola nel paradigma delle "quattro V[51]" in riferimento al Volume (inerente alla dimensione dei dati generati e acquisiti) alla Varietà (con riguardo alle numerose tipologie dei dati disponibili, tra i quali, oltre ai dati strutturati tradizionali, vi sono anche dei dati semi-strutturati e non strutturati) alla Veridicità (afferente alla certezza dell'elaborazione fornita dal calcolo matematico) e alla Velocità delle operazioni di trattamento.
Alle quattro caratteristiche se ne è aggiunta un'altra, ovvero il Valore che i dati assumono allorquando vengono elaborati ed analizzati. Elaborare i dati è stato, quindi, riconosciuto come elemento di valore consentendo di estrarre nuove informazioni che possono contribuire all'efficienza e alla qualità dei processi produttivi tradizionali[52].
Nell'evoluzione tecnologia introdotta dall'Industria 4.0 i *Big Data* fanno propria una posizione di centralità poiché, grazie alle *"moderne pratiche di analytics e alle tecnologie che le consentono, l'enorme mole di dati"*[53] che i contesti lavorativi producono "*è trattata in modo da ottenere informazioni utili a fini decisionali"*[54].

[50] Altre definizioni di "*Big Data*" sono fornite dal Parlamento europeo nella Risoluzione del 14 marzo 2017 sulle implicazioni dei *Big Data* per i diritti fondamentali: *privacy*, protezione dei dati, non discriminazione, sicurezza e attività di contrasto (2016/2225(INI)) e la comunicazione "*Una strategia europea per i dati*" della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni del 19.02.2020; Article 29 WorkinParty, Opinion 3/2013 on purpose limitation: "*The exponential growth both in the availabilit and in the automated use of information: it refers to gigantic digital dataset help by corporation (…) which are then extensively analysed (…) using computer algorithms*"; ENISA, Privacy by design in big data. An overview of privacyenhancing technologies in the era of big data analytics, 2015: "*The term "big data analytics" refers to the whole data management lifecycle of collection, organizing and analysing data to discover patterns, to infer situations or states, to predict and to understand behaviours*"; Consiglio d'Europa del 23.01.2017, Raccomandazione CM/Rec(2010)13 del Comitato dei Ministri del Consiglio d'Europa agli Stati membri sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale nel contesto delle attività di profilazione, del 23 novembre 2010 e le Linee guida sulla protezione delle individuali con riferimento al trattamento dei dati personali in un mondo di big data: "*In terms of data protection (…) the definition of Big Data therefore encompasses both Big Data anche Big Data Analytics".*
[51] Cfr. Zeno-Zencovich V., Giannone Codiglione G., *Ten legal perspective on the "big data revolution*", in *Concorrenza e Mercato*, vol. 23, 2016, p. 57; Valenduc G., Vendramin P., *Work in the digital economy: sorting the old from the new*, ETUI Working Paper, n. 3, 2016, p. 20; Mantelero A., *Big Data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo,* in *Diritto dell'Informazione e dell'Informatica*,n. 1, 2012, pp. 135-145; Rota A, *Rapporto di lavoro e big data analytics: profili critici e risposte possibili*, in *Labour & Law Issues (LLI),* 2017, vol.3,pp. I.34 ss.
[52] Così nell' Indagine Conoscitiva sui *Big Data* del 2018 conclusasi nel 2020 condotta dall'Autorità Garante della Concorrenza e Del Mercato (AGCM), dell'Autorità per le Garanzie nelle Comunicazioni (AGCOM) e dal Garante per la Protezione Dei Dati Personali.
[53] Dagnino E., *Dalla fisica all'algoritmo: una prospettiva di analisi giuslavoristica*, ADAPT University Press, 2019, p. 35.
[54] Dagnino E., *Dalla fisica all'algoritmo: una prospettiva di analisi giuslavoristica*, ADAPT University Press, 2019, p. 35.

Si avvia, pertanto, l'era della *Data Analysis* o *Big Data Analytics*[55], ovvero dell'analisi di dati (personali e non) con l'obiettivo di "*realizzare previsioni e proiezioni riferibili a una collettività che non ha consapevolezza e autopercezione di sé come parte di un gruppo*"[56] e con la finalità di guidare le decisioni inerenti alle persone[57].

4. Modelli di analisi

Mediante i dati acquisiti dai *software* in uso per la gestione dei lavoratori o per l'esecuzione della prestazione, possono essere organizzati *database* afferenti ai lavoratori, ulteriormente implementati con i dati raccolti nei "luoghi di lavoro digitali".

Ciò consente di svolgere elaborazioni definite *Data Analysis* che identificano il processo che pianifica, raccoglie, ispeziona, analizza dati al fine di individuare informazioni utili al processo decisionale.

L'uso della *Data Analysis* per la gestione dei lavoratori si è dimostrata efficace per migliorare le prestazioni aziendali riducendo i costi, migliorando la qualità nel reclutamento, ottimizzando la gestione dei talenti, implementando il coinvolgimento dei dipendenti e, in generale, aumentando la produttività.

Le stesse analisi sono in grado di offrire uno spaccato delle relazioni sviluppate all'interno di un'organizzazione.

Per esempio, i sistemi di *Digital Workplace* sono in grado di restituire dei *report* contenenti informazioni sul grado di interazione intrattenute tra i dipendenti, sulle discussioni a cui i singoli hanno partecipato o sul livello di formazione conseguito.

Le *Data Analysis,* in riferimento alla tipologia di dati analizzati, possono essere distinte nelle seguenti tipologie:

- *Peolple Analytics, Workforce Analytics e HR Analytics*: in questo caso si fa riferimento ad analisi che attengono a dati di persone/lavoratori.
- *Text Mining*, ovvero tecniche che analizzano il linguaggio utilizzato da singoli soggetti in documenti o all'interno di discorsi. Tali elaborazioni possono essere compiute mediante metodiche NLP (*Natural Language Processing*), ovvero analisi che interessano il linguaggio naturale, o NER (*Named Entity Recognition*), ossia processi di estrazione di informazioni da documenti non strutturati.
- *Sentiment Analysis* (o *Opinion Mining*). Queste analisi consistono in un'elaborazione computazionale di opinioni, sentimenti, valutazioni, apprezzamenti, attitudini ed emozioni delle persone.

---

55 Definizione ritrovabile in ENISA, *Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analyti*cs, 2015: "*The term "big data analytics" refers to the whole data management lifecycle of collection, organizing and analysing data to discover patterns, to infer situations or states, to predict and to understand behaviours*"; Consiglio d'Europa del 23.01.2017, Raccomandazione CM/Rec(2010)13 del Comitato dei Ministri del Consiglio d'Europa agli Stati membri sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale nel contesto delle attività di profilazione, del 23 novembre 2010 e le Linee guida sulla protezione delle individuali con riferimento al trattamento dei dati personali in un mondo di *Big Data*: "*In terms of data protection (…) the definition of Big Data therefore encompasses both Big Data anche Big Data Analytics"*. In merito Donini A., *Tecniche avanzate di analisi dei dati e protezione dei lavorator*i, in *Diritto delle Relazioni Industriali (DRI),* n. 1, 2018, p. 223; Valenduc G., Vendramin P., *Work in the digital economy: sorting the old from the new*, ETUI Working Paper, n. 3, 2016, p. 20 i quali affermano che "*big data collection and analysis has implication in terms of surveillance and monitoring in the workplace and tracking of employee activities*". Cfr. Rota A.*, Rapporto di lavoro e big data analytics: profili critici e risposte possibili*, in *Labor & Law Issues (LLI)*, vol.3, n.1, 2017 pp. I 33 ss.

56 Donini A., *Tecniche avanzate di analisi dei dati e protezione dei lavoratori*, in *Diritto delle Relazioni Industriali*, n. 1, 2018, p. 225; Mantelero A., *Rilevanza e tutela della dimensione collettiva della protezione dei dati personali*, in *CI/Europa*, n. 1, 2015, pp. 146-147.

57 Cfr. Dagnino E., *People Analytics: lavoro e tutele al tempo del management tramite big data,* in *Labor & Law Issues (LLI)*, vol. 3, n. 1, 2017, p. I7.

Le elaborazioni possono essere integrate nel sistema operativo utilizzato dai lavoratori (come nel caso di alcune *Digital Workplace*[58]*)* o supportate da un applicativo esterno.
Il processo di *Data Analysis* si articola, generalmente, in fasi distinte che si sviluppano nelle seguenti operazioni:

- raccolta dati. I dati acquisiti comportano la creazione di "*database*" che archiviano informazioni afferenti ai lavoratori. In tale fase è possibile avviare anche un processo di "pseudonimizzazione"[59], anche se risulta complesso realizzare un *set* di dati che risulti realmente "anonimo"[60] al termine dell'elaborazione. Le interazioni che si realizzano durante l'elaborazione possono, infatti, consentire di identificare un soggetto o di interferire sui suoi diritti[61].
- Analisi dei dati. L'elaborazione avviene mediante il supporto di algoritmi o tecniche di IA al fine di individuare modelli (definiti *pattern)* di correlazione.
  Sebbene la ricerca di corrispondenze per definire schemi sia una procedura utile al fine di valutare il grado di relazione tra distinte variabili, si deve tenere presente che l'analisi definisce esclusivamente il grado in cui queste sono legate.
  Un fattore estraneo a quelli considerati potrebbe, quindi, influenzare la relazione tra le variabili, agendo da "mediatore". Per tale ragione, nell'ambito dei rapporti di lavoro è importante prendere in considerazione quanti più dati possibili da sottoporre al vaglio algoritmico prima di trarre conclusioni. Il rischio è, altrimenti, quello di assumere una decisione non informata che ha un impatto reale sui lavoratori[62].
- Classificazione dei risultati ottenuti. I risultati dell'analisi possono essere organizzati mediante la creazione di *rating* che permettono di classificare gli *output* in un sistema ordinato in relazione allo scopo preposto dall'organizzazione.

Al termine di questa breve introduzione sulle differenti tecniche di analisi, si procede ad illustrare nello specifico le caratteristiche di ogni tecnica.

---

58 Per esempio, Microsoft Viva è dotata di propri moduli di analisi.
59 Per l'Art. 4 n. 5) Regolamento UE 2016/679 (GDPR) la "*pseudonimizzazione è il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile*". L'utilizzo di tecniche di pseudonimizzazione "*può ridurre i rischi per gli interessati" (*Considerando 28 GDPR*), anche se "i dati personali sottoposti a pseudonimizzazione, (…), dovrebbero essere considerati informazioni su una persona fisica identificabile* (Considerando 26 GDPR). I dati pseudo anonimi restano, quindi, dati potenzialmente identificabili.
60 Un dato anonimo è un' "*informazione originariamente non associabile ad uno specifico interessato*" (cfr. Garante 23 gennaio 1998, in *Bollettino* n. 3, pag. 24 [doc. web n. 39568]) e che, quindi "*non consentano di identificare, anche indirettamente, gli interessati*" (cfr. Garante 14 giugno 2001, in *Bollettino* n. 21, pag. 43 [doc. web n. 41782]).
61 In merito Article 29 Working Party, opinion 4/2007 *on the concept of personal data*, pp. 11-12; Risoluzione del Parlamento Europeo del 14 marzo 2017, punto 5; Donini A., *Tecniche avanzate di analisi dei dati e protezione dei lavoratori*, in *Diritto delle Relazioni Industriali (DRI),* n. 1, 2018, p. 229.
62 Cfr. Dagnino E., *People Analytics: lavoro e tutele al tempo del management tramite big data,* in *Labor & Law Issues (LLI)*, vol. 3, n. 1, 2017, p. 31.

4.1. *People Analytics*

Le *People Analytics*[63] sono state definite come la "*raccolta e analisi di grandi quantità di dati per identificare modelli di atteggiamento e prevedere comportamenti di gruppi e comunità*"[64].

Tali tecniche hanno assunto un ruolo centrale per le strategie di *Human Resource* (*HR*) e risultano strumenti capaci di acquisire, correlare e interpretare dati di lavoratori (o candidati tali) al fine di ottenere un'analisi dei singoli e delle loro interazioni con l'organizzazione per il raggiungimento degli obiettivi prefissati.

Le *People Analytics* sono, quindi, impiegate per "*misurare, registrare e comprendere le prestazioni dei dipendenti, gli aspetti inerenti alla pianificazione della forza lavoro, la gestione dei talenti e la gestione operativa*" consentendo di condurre "*analisi in tempo reale nel momento del bisogno nel processo aziendale (...)"* e ciò permette "*di comprendere più a fondo le questioni e di ottenere informazioni direttamente applicabili al business*" [65].

L'attività di *People Analytics* viene, così, denominata *HR Analytics* quando i dati assumono un ruolo centrale per le strategie nell'ambito della gestione delle risorse umane o *Workforce Analytics* nel caso in cui si faccia riferimento a un'analisi relativa all'intera forza lavoro[66].

I termini si riferiscono, dunque, a pratiche manageriali di gestione della forza lavoro strettamente connesse alle tecnologie *ICT* sia per la fase di acquisizione che per la successiva elaborazione di dati, finalizzate all'abilitazione di processi decisionali[67].

Tali tecniche sono, quindi, "*sistemi di gestione delle risorse umane che ricavano informazioni in merito ai lavoratori sulla base dell'analisi di rilevanti quantità di dati dallo svolgimento dell'attività lavorativa (sistemi di monitoraggio dell'attività lavorativa, di registrazione delle presenze o di geolocalizzazione), oppure reperiti in diversi contesti digitali (come le banche dati pubblicamente accessibili, i social networks, o i motori di ricerca*"[68].

Le ricerche condotte sulle *People Analytics* hanno dimostrato come questa tecnologia sia dotata di una potenzialità di analisi capace di restituire una descrizione basata non su informazioni statiche e frammentarie, bensì su un flusso di dati che quantifica e qualifica i comportamenti – soprattutto digitali – computando le informazioni.

Tali tecniche permettono, quindi, di acquisire dati sull'attività lavorativa di singoli o gruppi, rielaborarle tramite algoritmi o sistemi di IA al fine di offrire "*soluzioni sintetiche (numeriche o percentuali) (…) capaci di disvelare parametri chiave relativi al personale in forza, come il tasso di dismissioni in una certa area (…), il livello di performance, il talento del singolo (…)*"[69].

---

[63] A riguardo Dagnino E., *People Analytics: lavoro e tutele al tempo del management tramite big data,* in *Labor & Law Issues (LLI),* vol. 3, n. 1, 2017, pp. 4 ss.; Rota A., *Rapporto di lavoro e big data analytics: profili critici e risposte possibili,* in *Labor & Law Issues (LLI)*, vol. 3, n. 1, 2017, pp. 34 ss..; Sitzia A., *Personal computer e controlli "tecnologici" del datore di lavoro nella giurisprudenza*, in *Argomenti di Diritto del Lavoro (ADL),* n. 3, 2017, pp. 804 ss.; Donini A., *Tecniche avanzate di analisi dei dati e protezione dei lavoratori*, in *Diritto delle Relazioni Industriali (DRI),* n.1, 2018; Ingrao A., *Data-Driven management e strategie collettive di coinvolgimento dei lavoratori per la tutela della privacy* in *Labour & Law Issues (LLI)*, vol.5, n. 2, 2019, pp. 222 ss.; Ingrao A, *Il Controllo a distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata*, Cacucci Editore, Bari, 2018, pp.179 ss.

[64] Linee guida sulla protezione delle individuali con riferimento al trattamento dei dati personali in un mondo di big data del Consiglio d'Europa del 23.01.2017.

[65] European Agency for Safety and Healt at Work, Documento di riflessione, *La SSL e il futuro del lavoro: vantaggi e rischi degli strumenti di intelligenza artificiale nei luoghi di lavoro*, p. 4, consultabile online su www. osha.europa.eu. In merito anche Collins, L., Fineman, D. R., Tshuchica, A., *People analytics: Recalculating the route», Deloitte Insights*, 2017, Disponibile *online*: https://www2.deloitte.com/insights/us/en/focus/human-capital-trends/2017/people- analytics-in-hr.html.

[66] Alcuni autori giungono a definire una "*Productivity app*" ove sarebbe lo stesso lavoratore a voler impiegare i dati raccolti dal datore di lavoro al fine di contraltare condizioni economiche e normative più vantaggiose (come premi di risultato). In merito Marazza M., *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore*), in *WP CSDLE "Massimo D'antona".it,* n. 300, 2016, pp. 8-9.

[67] In tal senso Dagnino E., *Dalla fisica all'algoritmo: una prospettiva di analisi giuslavoristica,* Adapt, University press, 2019, p. 36.

[68] Ingrao A, Donini A., *Algoritmi e lavoro*, in *Labour Law Community* del 25 maggio 2022, p. 8 consultabile *online* https://www.labourlawcommunity.org/ricerca/algoritmi-e-lavoro/.

[69] Ingrao A., *Il controllo a distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata*, Cacucci Editore, Bari, 2018, p. 180.

La capacità di analisi di dette pratiche è in grado di disvelare anche l'insorgere di situazioni patologiche in taluni soggetti[70] o manifestazioni di *stress* lavoro correlate[71].

Secondo i dati riportati dal documento "*Commission staff working document*[72]*"* della Commissione Europea, nel 2019 il 12% delle imprese europee usava strumenti informatici per la gestione o la sorveglianza dei dipendenti, l'11,8% per determinare il contenuto o l'intensità del lavoro, l'8,2% per monitorare le *performance* dei lavoratori. Questa tecnologia risulta essere, quindi, già diffusa e accessibile alle organizzazioni europee e italiane[73], come emerge dallo studio condotto dall'Università degli Studi di Modena e Reggio Emilia[74] che ha indagato su "*Le People Analytics nelle imprese italiane: stato dell'arte e prospettive*" al fine di comprendere l'attuale adozione, le potenzialità e gli sviluppi futuri[75] delle *People Analytics* nelle aziende nazionali.

La ricerca ha coinvolto un campione di 490 *HR Manager* italiani, a cui è stato domandato il grado di utilizzo delle *People Analytics* nei processi di gestione del personale all'interno delle aziende ove operano e la loro opinione sulla futura applicazione di tali tecniche.

Lo studio, in primo luogo, ha analizzato la diffusione dei sistemi informativi del personale (gli *Human Resources Information Systems - HRIS*) e l'eventuale integrazione delle informazioni estratte da tali sistemi con dati provenienti da altre fonti.

A riguardo, la grande maggioranza degli intervistati (70%) ha dichiarato che l'impresa presso cui è impiegato possiede un sistema informativo e, di questa maggioranza, circa il 40% ha precisato che è stato adottato un *HRIS* unico e integrato[76].

---

[70] In merito l'impiego da parte di Inail di tecniche di Data Analyst per verificare la salubrità dei luoghi di lavoro cfr. De Padova C., *La nuova frontiera dell'IT (Information Technology)*, in *Rivista degli infortuni e delle malattie professionali*, 2013, n. 1-2, pp. 247 ss.

[71] Cfr. Curzi Y., Pistoresi B., Fabbri T, *Understanding the stressful implications of remote e-working: Evidence from Europe*, Working paper, DEMB WORKING PAPER SERIES, Dipartimento di Economia Marco Biagi - Università di Modena e Reggio Emilia, 2020, pp. 1-17; Del Giglio I., *Valutazione della performance mediante tecniche di People Analytics. Privacy in employment, controllo o innovazione?*, *in Journal of Ethics and Legal Technologies (JELT)*, n. 11, 2021, pp. 103-137.

[72] Documento preparato dalla Commissione Europea per la consultazione delle parti sociali sulla digitalizzazione, Commissione Europea, *Commission staff working document*, C (2021), 4230 final; EU-OSHA (2020). European Survey of Enterprises on New and Emerging Risks (ESENER) 2019.

[73] Da una ricerca riportata nel Documento di riflessione della European Agency for Safety and Healt at Work intitolato "*La SSL e il futuro del lavoro: vantaggi e rischi degli strumenti di intelligenza artificiale nei luoghi di lavoro"* si osserva come oggigiorno nelle aziende internazionali circa il 40 % delle attività di gestione delle risorse umane utilizza applicazioni IA al fine di effettuare analisi sui lavoratori in forza mediante tecniche di *People Analytics*. Lo studio osserva come "*queste aziende hanno sede principalmente negli Stati Uniti, ma si stanno affacciando anche alcune organizzazioni europee e asiatiche. Secondo un'indagine di PwC* (ndr. del 2018), *sempre più aziende in tutto il mondo iniziano a capire il valore dell'IA nel supportare la gestione della forza lavoro. Da una relazione emerge che il 32 % dei dipartimenti di gestione del personale nelle aziende tecnologiche o di altri settori sta riorganizzando il proprio assetto con l'aiuto dell'IA con l'intento di ottimizzare l'adattabilità e l'apprendimento per integrare al meglio tutte le informazioni raccolte attraverso il feedback dei dipendenti e la tecnologia. (…) Una relazione di Deloitte mostra che il 71 % delle aziende internazionali considera la People Analytics una priorità assoluta per le proprie strutture, in grado non solo di poter fornire buone indicazioni commerciali, ma anche di gestire i cosiddetti «people problems»*". In *La SSL e il futuro del lavoro: vantaggi e rischi degli strumenti di intelligenza artificiale nei luoghi di lavoro* p. 4., consultabile online su www.osha.europa.eu.

[74] L'indagine "*Le People Analytics nelle imprese italiane: stato dell'arte e prospettive"* è stata condotta nell'ambito del Progetto di ricerca interdisciplinare "*Framing employee attitudes and digital behaviors to support data-driven human resource management*" e finanziata dal Fondo di Ateneo per la Ricerca 2017 dell'Università degli Studi di Modena e Reggio Emilia.

[75] L'arco temporale considerato è di tre anni.

[76] Ad esempio Zucchetti, Successfactors, Kenexa, Workday.

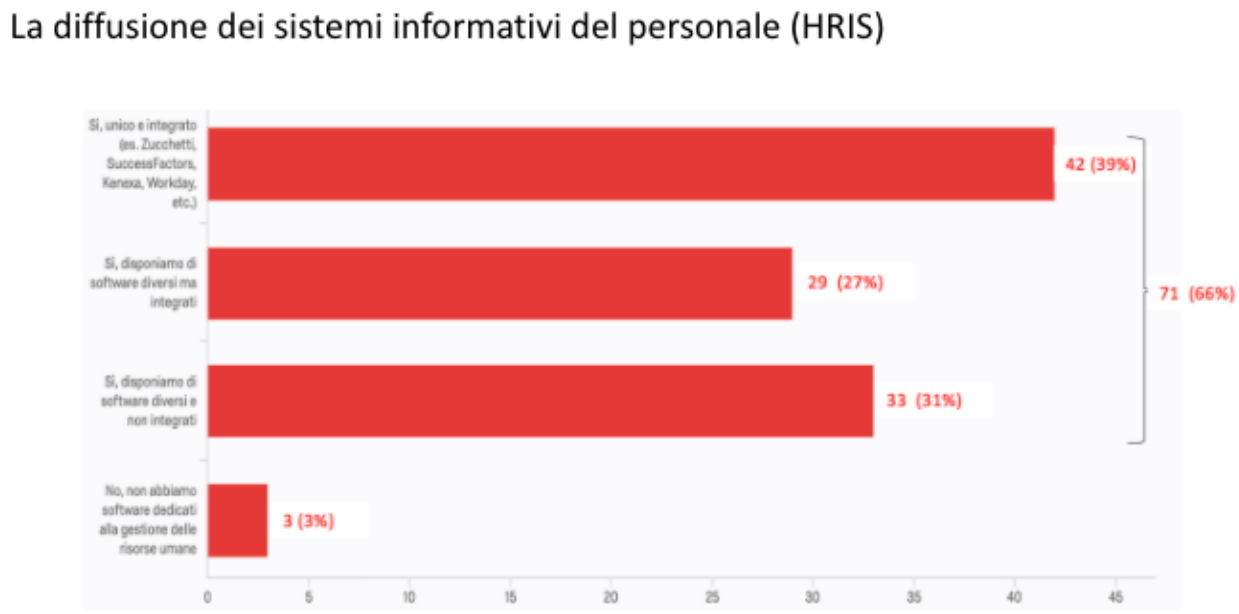


Figura 1: diagramma rappresentante la diffusione dei sistemi formativi del personale (*HRIS*) dalla presentazione dello studio "*Le People Analytics nelle imprese italiane: stato dell'arte e prospettive*"

Gli ambiti in cui vengono attualmente utilizzati i sistemi informativi del personale sono ampi ed eterogeni, variando dalla retribuzione all'analisi dei costi, dalla valutazione delle prestazioni alla selezione e formazione.
Da ciò lo studio ha dedotto come vi sia in atto una progressiva digitalizzazione di tutti i processi di gestione delle risorse umane[77].

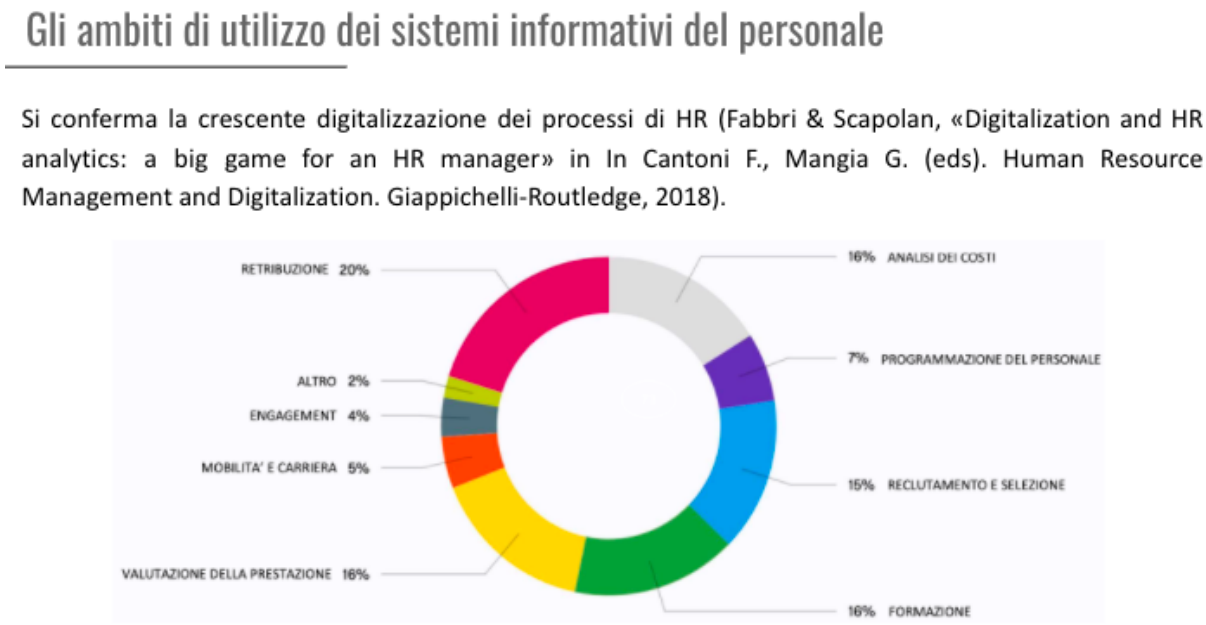


Figura 2: diagramma rappresentante gli ambiti di utilizzo dei sistemi formativi del personale (HRIS) dalla presentazione dello studio "*Le People Analytics nelle imprese italiane: stato dell'arte e prospettive*"

La maggioranza degli intervistati (il 62%) ha dichiarato di avere accesso anche ad altre fonti di informazioni, esterne ai HRIS. In particolare, i dati "esterni" vengono acquisiti principalmente da *software*

[77] Fabbri T., Scapolan A. C., *Digitalization and Hr Analytics: A big game for an HR manager*, in Cantoni F., Mangia G. (a cura di), *Human Resource Management and Digitalization*, Giappichelli Routledge, 2018, pp. 243-254.

aziendali o sistemi di gestione, come i sistemi ERP o CRM (nella misura del 24%). Un'ulteriore fonte di dati "esterni" ai HRIS sono i *software* di posta elettronica (quali *Outlook, Gmail*, per il 23%).
Infine, in misura minoritaria (15%) le informazioni vengono apprese da strumenti *social* (per es. *LinkdIn)*, piattaforme collaborative e *Digital Workplace* (come *Facebook Work, Slack, Trello, G Suite*).

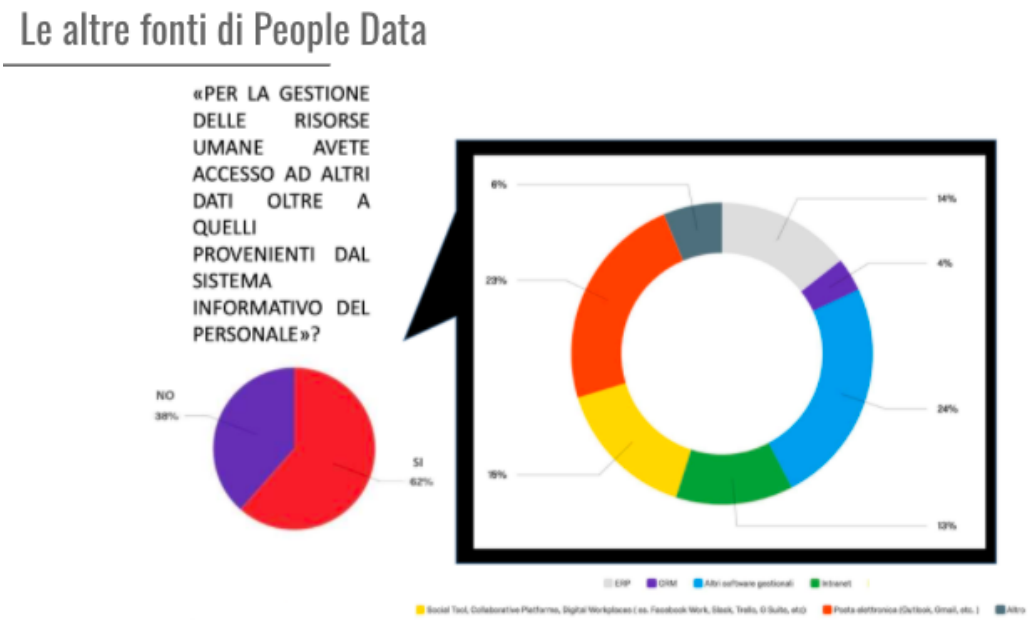


Figura 3: diagramma rappresentante le fonti da cui vengono acquisiti i dati per le analisi di People Analytics, dalla presentazione dello studio "*Le People Analytics nelle imprese italiane: stato dell'arte e prospettive*"

Nelle imprese che usufruiscono di più fonti di acquisizione di dati afferenti ai lavoratori, la maggioranza (circa il 57%) integra le informazioni in un unico *database*, anche mediante procedure completamente automatizzate.

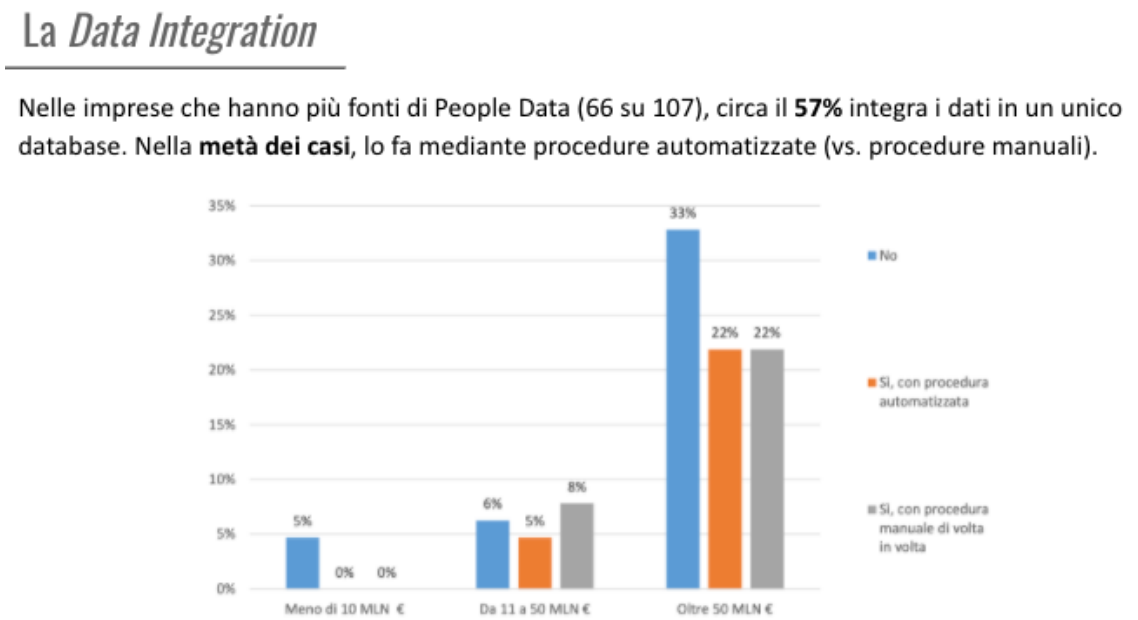


Figura 4: diagramma rappresentante il livello di integrazione delle fonti per le analisi di *People Analytics*, dalla presentazione dello studio "*Le People Analytics nelle imprese italiane: stato dell'arte e prospettive*"

I sistemi informativi di gestione del personale (HRIS) risultano, inoltre, equamente distribuiti nelle imprese indipendentemente dalla dimensione.

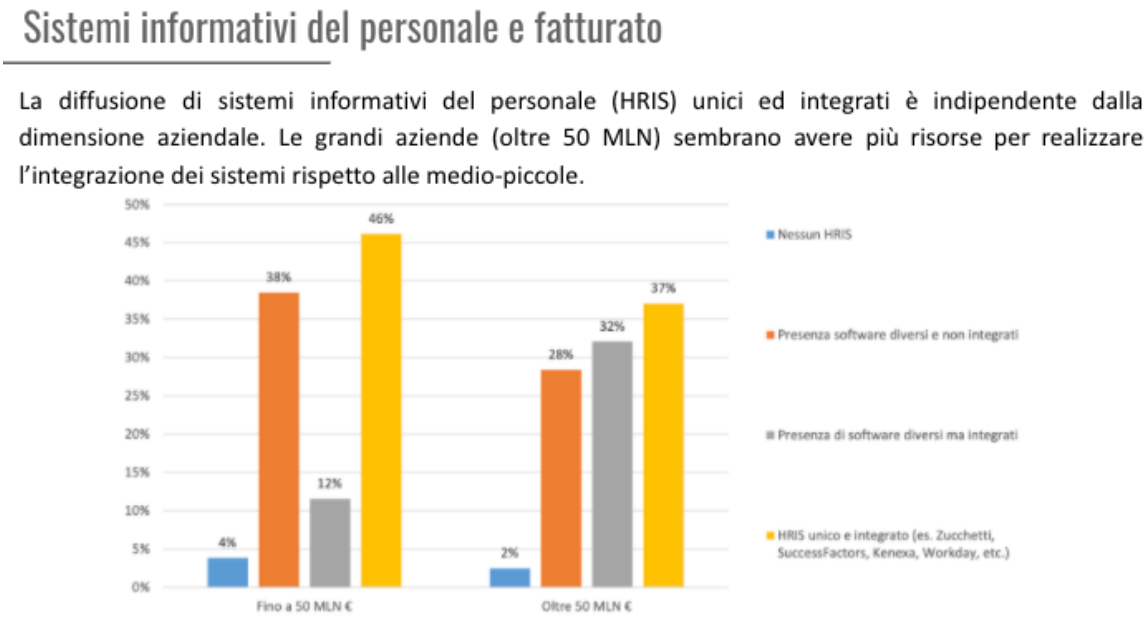
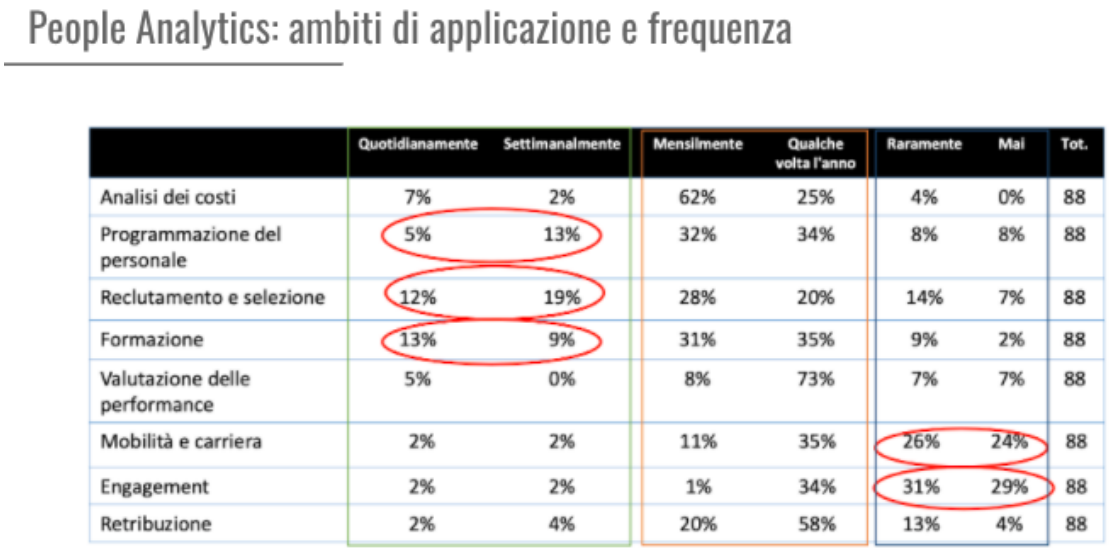


Figura 5: diagramma rappresentante la diffusione dei sistemi *HRIS*, dalla presentazione dello studio "*Le People Analytics nelle imprese italiane: stato dell'arte e prospettive*"

Gli ambiti in cui vengono maggiormente impiegati sistemi di *People Analytics* sono quelli afferenti alla misurazione dell'efficienza (45 %, tra cui rientra il processo di assunzione e selezione dei candidati idonei) e all'efficacia dei processi di gestione delle risorse umane (35%, tra cui viene indicata la valutazione della *performance*).



	Quotidianamente	Settimanalmente	Mensilmente	Qualche volta l'anno	Raramente	Mai	Tot.
Analisi dei costi	7%	2%	62%	25%	4%	0%	88
Programmazione del personale	5%	13%	32%	34%	8%	8%	88
Reclutamento e selezione	12%	19%	28%	20%	14%	7%	88
Formazione	13%	9%	31%	35%	9%	2%	88
Valutazione delle performance	5%	0%	8%	73%	7%	7%	88
Mobilità e carriera	2%	2%	11%	35%	26%	24%	88
Engagement	2%	2%	1%	34%	31%	29%	88
Retribuzione	2%	4%	20%	58%	13%	4%	88

Figura 6: tabella riassuntiva riportante gli ambiti di diffusione delle tecniche di *People Analytics*, dalla presentazione dello studio "*Le People Analytics nelle imprese italiane: stato dell'arte e prospettive*"

Per quanto riguarda i tipi di analisi effettuate sui dati dei lavoratori, le elaborazioni svolte con maggior frequenza sono quelle descrittive, ovvero le analisi destinate a indicare cosa avviene all'interno di un'impresa rappresentando l'andamento in riferimento ad una "variabile di interesse" (come il livello di assenteismo per area geografica).

Al secondo posto vi sono le analisi diagnostiche, ovvero quelle volte e spiegare il perché è accaduto un determinato evento.
In questo caso, i dati vengono analizzati per comprendere il *trend* di una "variabile d'interesse" (ad esempio, l'effetto dell'anzianità aziendale sul livello di assenteismo).
Infine, le meno utilizzate sono le analisi predittive, ossia quelle destinate a prevedere cosa accadrà, provando a delineare la tendenza di una "variabile d'interesse" (come il livello di assenteismo per area geografica nell'anno successivo).

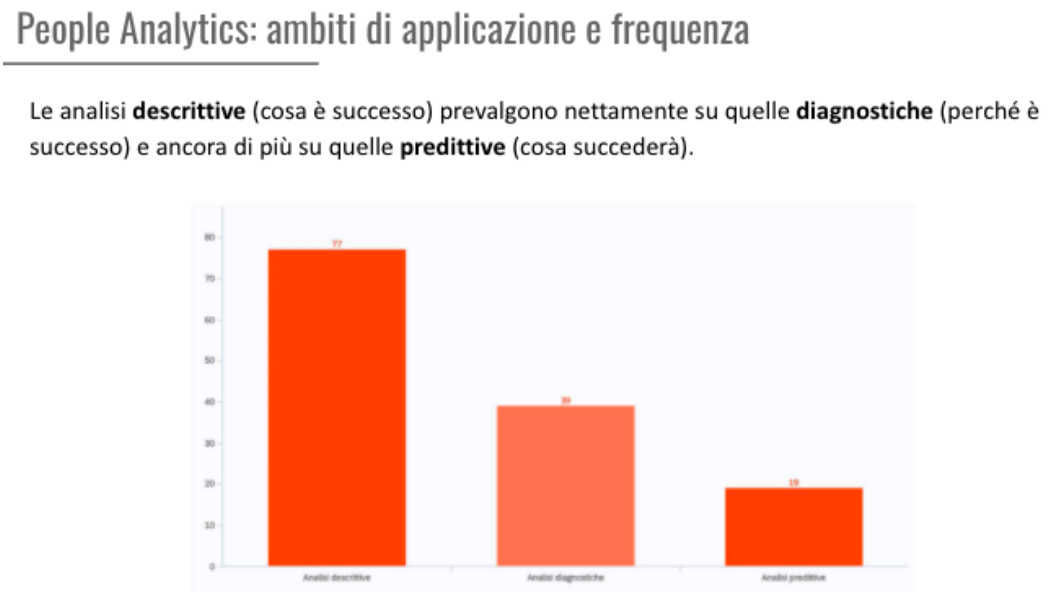


Figura 7: diagramma rappresentante gli ambiti di applicazione delle tecniche di *People Analytics*, dalla presentazione dello studio "*Le People Analytics nelle imprese italiane: stato dell'arte e prospettive*"

Gli strumenti prevalentemente utilizzati per compiere *Data Analysis* risultano essere nella maggior parte dei casi *software* esterni e ulteriori rispetto a quelli impiegati per la gestione del personale, che si avvalgono di pagine di elaborazione statistica come "*Excel*".
Meno diffuso è, invece, l'impiego di moduli aggiuntivi ai *software* gestionali impiegati (come gli HRIS o i CRM) e gli applicativi statistici programmabili per l'analisi dei dati (quali possono essere STATA, SPSS o R). Anche in quest'ultimi casi, si parla di *software* o applicazioni esterni rispetto a quelli destinati alla funzione organizzativa dei lavoratori.

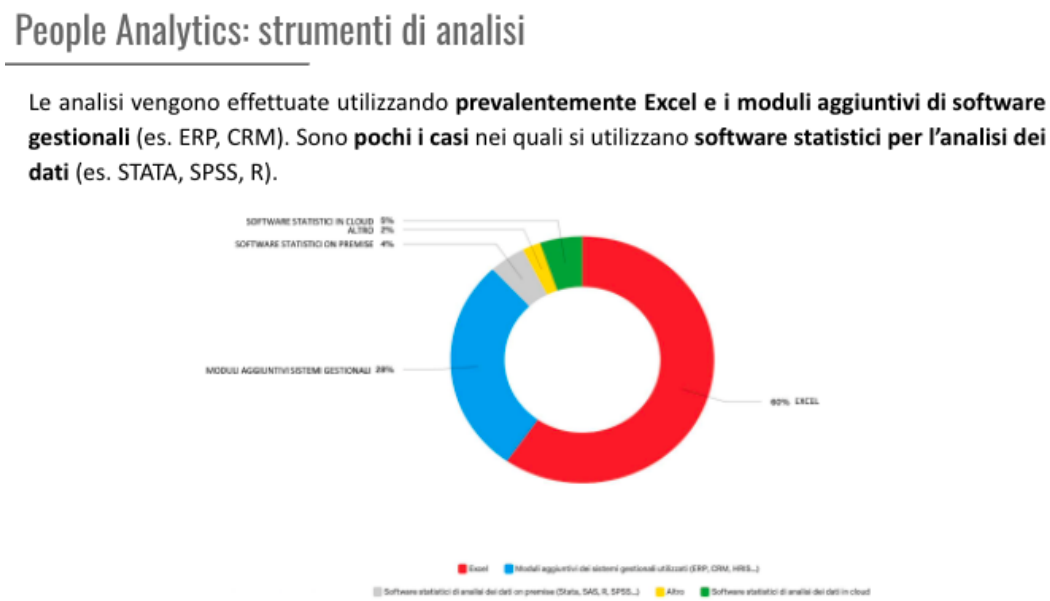


Figura 8: diagramma rappresentante gli strumenti di analisi impiegati, dalla presentazione dello studio "*Le People Analytics nelle imprese italiane: stato dell'arte e prospettive*"

In riferimento allo sviluppo e alla diffusione di tecniche di *People Analytics*, la maggior parte degli HR *manager* intervistati ha dichiarato che il loro sviluppo è "significativo" o "molto significativo" e che, conseguentemente, sperimenteranno e implementeranno tali tecniche nei prossimi tre anni per la gestione dei lavoratori.

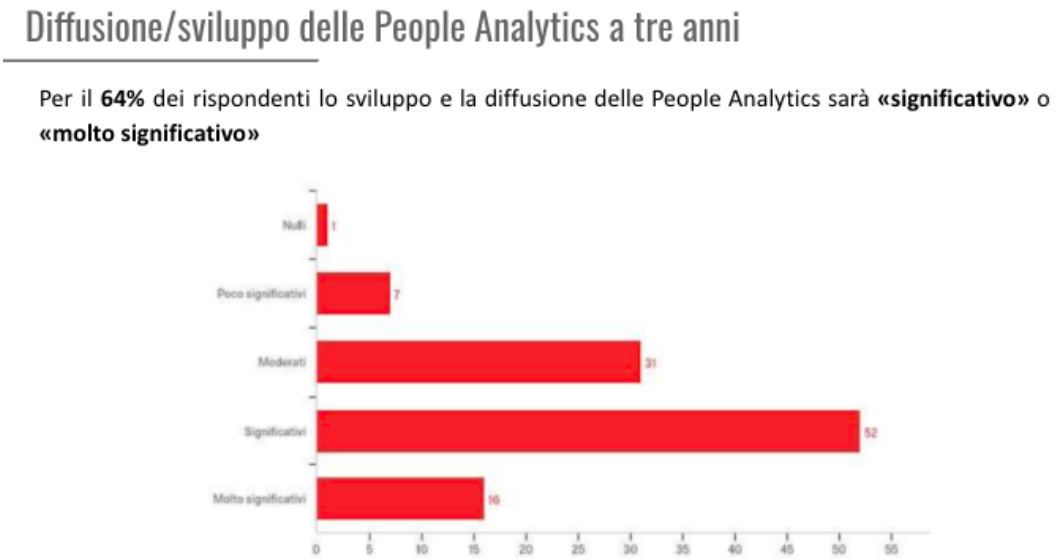


Figura 9: diagramma rappresentante la diffusione prevista delle tecniche di *People Analytics* nei prossimi tre anni, dalla presentazione dello studio "*Le People Analytics nelle imprese italiane: stato dell'arte e prospettive*"

Quasi la metà degli intervistati ritiene, infine, che nei prossimi tre anni le analisi predittive saranno le elaborazioni maggiormente praticate.

Figura 10: diagramma rappresentante la rilevanza delle tecniche di *People Analytics* nei prossimi tre anni, dalla presentazione dello studio "*Le People Analytics nelle imprese italiane: stato dell'arte e prospettive*"

Lo studio evidenzia, quindi, come la diffusione di sistemi informativi del personale (HRIS) sia un elemento comunemente impiegato nelle imprese, indipendente dalla loro dimensione.
Diversamente, il valore economico del fatturato aziendale influisce sugli investimenti per integrare sistemi di *People Analytics,* favorendo le imprese di grandi dimensioni (ovvero quelle che presentano un fatturato di oltre 50 milioni) che, possedendo maggiori risorse, integrano tali sistemi in misura maggiore per la gestione dei lavoratori.
È, inoltre, emerso come la pratica e l'esperienza dei *manager HR* nell'utilizzare abitualmente sistemi *Data Driven*[78] si differenzi notevolmente a seconda dei settori aziendali presi in considerazione, previlegiando l'utilizzo di queste tecniche per i processi di selezione e reclutamento, il cui impiego è giornaliero o settimanale.
In altri ambiti, come l'analisi sui costi, il calcolo delle retribuzioni e la valutazione delle *performance*, vengono adoperati mensilmente o annualmente.
L'indagine pone, quindi, in evidenza come i sistemi di *People Analytics* non solo siano già in uso, ma risultino anche in progressivo implemento presso le imprese italiane in differenti settori.

A febbraio 2022 è stata condotta la seconda edizione dello studio, coinvolgendo circa 100 *HR manager* di imprese italiane di diverse dimensioni, e i risultati sono stati illustrati a luglio 2022.
Il questionario, che è stato sottoposto alle imprese, era composto da 47 domande suddivise in 5 sezioni relative al profilo aziendale, agli HRIS in uso, alle finalità e ambiti di applicazione delle *People Analytics*, agli strumenti e alle tecniche impiegati per elaborare i dati, nonché ai soggetti coinvolti e alle competenze necessarie per il loro utilizzo. Infine, è stata indagata la prospettiva di sviluppo delle *People Analytics* nei prossimi tre anni.

[78] Cfr. Politecnico di Milano, *White Paper*. Osservatorio *HR Innovation Practice* (2016). "*HR Analytics & Big Data Driven Innovation: cosa significa e come impostare una roadmap di innovazione*". In collaboration with Cornerstone; Ingrao A., *Data-Driven management e strategie collettive di coinvolgimento dei lavoratori per la tutela della privacy* in *Labour & Law Issues (LLI),* vol.5, n. 2, 2019, pp. 222 ss.

I soggetti rispondenti sono stati nella prevalenza *HR manager* che lavorano in aziende di grandi dimensioni (più di 250 dipendenti e con fatturato di oltre 50 milioni di euro), equamente distribuite tra industria manifatturiera e settori di servizio.

L'indagine in riferimento alla diffusione dei sistemi informativi per la gestione del personale, quali gli HRIS, ha evidenziato che il dato relativo all'utilizzo di sistemi unici o integrati, rispetto alla prima *survey*, ad oggi interessa un numero inferiore di aziende: circa il 55% rispetto il precedente 66%. Emerge, dunque, la maggiore rilevanza di sistemi informativi "a mosaico" ovvero l'impiego di *software* differenti in relazione ai vai processi di gestione del personale.
In particolare, le imprese di grandi dimensioni si affidano più frequentemente a diversi *software* gestionali, ma -al contempo- dispongono di maggiori risorse per integrarli in un sistema unico, qualora risultasse necessario.
Diversamente, le PMI, si affidano prevalentemente a sistemi unici e integrati di gestione del personale.
È, inoltre, emerso che per le PMI esiste una soglia dimensionale sotto la quale non conviene investire in HRIS.

L'utilizzo dei sistemi informativi (quali gli HRIS) risulta diffuso in tutti gli ambiti di gestione del personale, confermando la progressiva digitalizzazione dei processi di HRM già evidenziato nella precedente indagine.

Dal nuovo sondaggio emerge, inoltre, che i dati oggetto di analisi provengono per la maggior parte dai sistemi di HRIS, quindi da fonti informative interne all'impresa.
A questi si affiancano altre fonti, sia interne che esterne all'azienda.
Tra le fonti interne figurano altri *software* gestionali, come i CRM e l'*Intranet* aziendale, mentre tra quelle esterne *Internet* e i *Social networks*.

Si è poi osservato che le imprese che dichiarano di accedere a fonti eterogenee per acquisire *People Data* (circa il 56% delle intervistate) integra i dati in un unico *database*. A procedere a tale integrazione sono soprattutto le imprese di grandi dimensioni (ovvero quelle con fatturato superiore a 50 milioni di euro).

I dati acquisiti sulle persone sono utilizzati dall'87% delle imprese rispondenti per elaborare delle analitiche, al fine di misurare l'efficacia, l'efficienza e l'impatto dei processi di HRM.
Il tasso di elaborazione di *People Analytics* risulta, quindi, leggermente aumentato rispetto alla prima *survey*, in cui si attestava sull'82%.

In relazione alla finalità di utilizzo delle *People Analytics,* nell'ultima *survey* risulta aumentata la percentuale di impiego di tali tecniche per misurare l'efficacia dei processi di gestione delle risorse umane (attualmente del 43%, mentre in precedenza si attestava al 35%).
È, invece, diminuita, rispetto all'edizione precedente, la percentuale di imprese che dichiara di utilizzare le *People Analytics* per misurare l'efficienza (ad oggi del 38%, mentre in precedenza era pari al 45%) e l'impatto dei processi di gestione delle risorse umane (ora del 18% a fronte del 20% indicato precedentemente).

In riferimento agli ambiti di applicazione e alla frequenza di utilizzo delle *People Analytics*, è stato rilevato che si effettuano elaborazioni con cadenza quotidiana/settimanale solo per la programmazione, la

formazione e il reclutamento/selezione del personale, ovvero nei tre ambiti di maggior utilizzo delle *People Analytics*.
Il mese o qualche volta l'anno rappresenta, invece, fascia di frequenza che totalizza il maggior numero di istanze su tutti gli ambiti di gestione delle risorse umane.

È, inoltre, emerso che meno del 20% dei rispondenti è completamente estraneo all'utilizzo di *People Analytics* negli ambiti decisionali tradizionali della gestione del personale, ad eccezione degli ambiti di *engagement/satisfaction* e di mobilità/carriera in cui rispettivamente il 60% e quasi il 40% dei rispondenti dice di usare raramente se non mai le *People Analytics*.

In riferimento al tipo di analisi che viene effettuato le più diffuse sono le analisi descrittive (55%) rispetto a quelle diagnostiche (26%) e predittive (18%).
Questi risultati confermano quanto emerso anche nella prima *survey*.

Vi è, inoltre, una conferma rispetto alla precedente indagine in merito alle tecniche di analisi utilizzate per elaborare *People Analytics*, venendo previlegiate tecniche di elaborazione statistica di base. Risultano, infatti, ancora poco diffuse tecniche di analisi più avanzate (impiegate solo dal 5% delle imprese rispondenti) e risultano non utilizzate tecniche di analisi molto avanzate (come il *data mining*).
Parimenti, gli strumenti di analisi impiegati sono prevalentemente *Excell* e moduli aggiuntivi di *software* gestionali (es. ERP, CRM), mentre sono sporadici i casi in cui vengono impiegati applicativi specifici per l'analisi dei dati (come STATA, SPSS e R).

Lo studio ha poi analizzato lo sviluppo delle *People Analytics* nei prossimi tre anni.
A riguardo, per il 79% dei rispondenti, lo sviluppo e la diffusione delle *People Analytics* sarà "significativo" o "molto significativo". Tale percentuale, nella prima edizione dell'indagine, era pari al 64%.
Sembra quindi essere maturata una maggiore consapevolezza in merito al ruolo che avranno le *People Analytics* nel prossimo futuro.

Rispetto alla prima *survey* risulta, inoltre, variata la distribuzione in riferimento alla diffusione delle *People Analytics* tra imprese di piccole e grandi dimensioni, emergendo una maggiore propensione a sviluppare progetti di *People Analytics* nelle aziende di grandi dimensioni.

Si conferma, inoltre, rispetto alla prima indagine, la percezione dell'elevata utilità delle *People Analytics* per il miglioramento sia dei processi di *HR* sia delle *performance* aziendali.

Quanto è emerso da questa seconda *survey* è che l'impiego delle *People Analytics* nel futuro prossimo risulta ancora un ambito in via di sviluppo sia dal punto di vista delle esperienze che delle competenze statistiche delle imprese coinvolte.

Quello che traspare dallo studio è che le *People Analytics* troveranno sempre maggiore applicazione in tutti gli ambiti della gestione delle risorse umane, con particolare attenzione all'*engagement* e alla soddisfazione dei dipendenti.

In riferimento agli acceleratori e agli ostacoli alla diffusione delle *People Analytics* è emerso che una cultura *data driven,* ove presente in azienda, è il maggior acceleratore per l'integrazione di tali tecniche. Viceversa, ove assente, rappresenta il principale ostacolo alla diffusione delle *People Analytics*.

Anche gli investimenti economici specifici in ambito di *People Analytics* agiscono positivamente come stimolo per l'implementazione dell'uso di tali analitiche. Al contrario, la mancanza di *budget* e le lacune tecnologiche ostacolano la diffusione delle *People Analytics*.
Gli elementi che potrebbero, quindi, favorire lo sviluppo futuro delle *People Analytics* ineriscono la formazione, la cultura *data driven*, la presenza di adeguate condizioni economiche, normative, tecnologiche e organizzative.
In particolare, per condizioni organizzative adeguate si intende la necessità di inserire le *People Analytics* all'interno di un sistema integrato di HRM che punti a valorizzare la strategicità delle risorse umane e il coinvolgimento delle stesse nelle decisioni di *business*.

Nel complesso, da questa seconda *survey*, è emerso che lo stato dell'arte delle *People Analytics* in Italia è sostanzialmente invariato negli ultimi due anni continuando a mostrare un'evoluzione crescente.
Gli *HR manager* italiani hanno consapevolezza delle potenzialità dei *People Data* il cui impiego risulta, però, nella pratica ancora limitato per frequenza, sofisticazione delle analisi e impatto percepito.

4.2. *Text Mining* mediante NLP (*Natural Language Processing*) e NER (*Named Entity Recognition*)

Le analisi di dati afferenti al linguaggio naturale dei lavoratori sono sempre più utilizzate dall'organizzazione, in particolare, per individuare competenze trasversali, definite "*soft skill*"[79].
Le *soft skill* integrano le abilità strettamente "tecniche" di un soggetto (dette "*hard skill*"[80]) e si riferiscono a caratteristiche legate alle doti comunicative o alle attitudini relazionali di un individuo fornendo criteri di valutazione atti a delineare l'idoneità al compimento di una prestazione o a eventuali prospettive di carriera[81].
Le competenze trasversali aiutano, dunque, le organizzazioni a migliorare le strategie di gestione dei lavoratori[82] consentendo, per esempio, di selezionare i candidati più in linea con i valori aziendali o maggiormente orientati a concretizzare gli obiettivi d'impresa. Nel contesto dell'Industria 4.0 l'apporto del singolo può essere, quindi, descritto dall'insieme delle sue abilità espresse, in senso ampio, dalle "*hard skill*" e "*soft skill*"[83].
La possibilità di individuale le *soft skill* di un lavoratore - non essendo ravvisabili elementi tecnici verificabili, per esempio, mediante il titolo di studio conseguito come accade con le *hard skill* - diviene possibile grazie al supporto fornito da tecniche di *Data Analysis* coadiuvate da processi algoritmici o di Intelligenza Artificiale (IA), come il *Machine Learning* o il *Deep Learning*[84].
Con la digitalizzazione acquisisce rilevanza la possibilità di valutare le abilità dei lavoratori.

---

[79] Cfr. Brollo M., *Disciplina delle mansioni (art. 3)* in Carinci F. (a cura di), *Commento al D.Lgs. 15 giugno 2015, n. 81: le tipologie contrattuali e lo jus variandi,* ADAPT University Press, ADAPT Labour Studies e-Book series, 2015, n. 48, pp. 29-34; Caruso B., *Strategie di flessibilità funzionale e di tutela dopo il Jobs Act: fordismo, post fordismo e industria 4.0*, in *Giornale di Diritto del Lavoro e di Relazioni Industriali (DLRI)*, n. 1, 2018, pp. 81 ss.
[80] Quali possono essere il grado di istruzione o le abilità linguistiche.
[81] Seghezzi F., *Le grandi trasformazioni del lavoro, un tentativo di periodizzazione. Appunti di ricerca*, Working Paper ADAPT, 2015, p. 193 per cui "*la natura stessa di tali competenze e dei sistemi produttivi farebbe sì che le mansioni specifiche per le quali si "acquisita" la prestazione del lavoratore siano sempre meno definite e definibili*".
[82] Cfr. Dagnino E., *Dalla fisica all'algoritmo: una prospettiva di analisi giuslavoristica*, ADAPT University Press, 2019, pp. 103-107.
[83] Cfr. Dagnino E., *Dalla fisica all'algoritmo: una prospettiva di analisi giuslavoristica*, ADAPT University Press, 2019, p. 105.
[84] Il cui funzionamento verrà illustrato al punto 5 del presente capitolo.

Ciò al fine di organizzare delle "tassonomie delle competenze"[85], strettamente connesse al "ruolo" svolto dal singolo, in modo da delineare le funzioni più idonee da espletare, anche in considerazione degli aspetti relazionali e collaborativi[86].
Per fare ciò, le imprese svolgono analisi su grandi quantità di dati che interessano, in particolar modo, il linguaggio naturale impiegato dai lavoratori in discorsi o documenti testuali.
La metodologia adottata si basa, quindi, su una scienza dei dati che, grazie ad algoritmi all'avanguardia o sistemi di IA, consente di svolgere un'analisi continua di informazioni provenienti da fonti eterogenee.
A riguardo si parla di NLP (*Natural Language Processing*) e di NER (*Named Entity Recognition*).
Le NLP e NER costituiscono tecniche di *Data Mining*[87], nello specifico di *Text Minig*[88], da intendersi quale sistema di IA che utilizza l'elaborazione del linguaggio naturale per trasformare il testo libero (non strutturato) tratto da documenti o *database* (come pagine *web*, *e-mail,* documenti *word*) in dati strutturati e organizzati.
In particolare, il NER consente di rilevare le unità lessicali in una sequenza di parole afferenti a un'entità predefinita determinando, in tal modo, la categoria a cui si riferisce la singolarità (es. persone, luoghi, organizzazioni.).
Si tratta, dunque, di un'analisi complessa di dati non strutturati volta a individuare una classificazione utile per il successivo processo decisionale.
Il supporto fornito dai sistemi di IA consente di individuare modelli (definiti *pattern)* di correlazione tra i termini impiegati nel linguaggio naturale così da identificare le *soft skill.*

4.3. *Sentiment Analysis* (o *Opinion Mining*)

La *Sentiment Analysis* (o *Opinion Mining)* è un ambito di studio che analizza, mediante tecniche di *Data Analysis,* opinioni, sentimenti, valutazioni, apprezzamenti, attitudini ed emozioni delle persone in riferimento ad alcune "entità".
Nell'ambito dei rapporti di lavoro, l'oggetto d'indagine dei dati acquisiti può essere non solo le capacità del singolo (*hard* o *soft*), ma anche il grado di integrazione con l'organizzazione o il livello di *stress*[89]/soddisfazione correlato alla mansione svolta.
Tali informazioni possono essere ottenute analizzando le caratteristiche personali dei soggetti, come opinioni o percezioni, mediante tecniche di *Sentiment Analysis.*
L'analisi avviene in maniera computazionale, ovvero avvalendosi di sistemi di IA, che permettono di elaborare un numero elevato di dati non strutturati ed eterogenei, quali sono i sentimenti o gli apprezzamenti manifestati dai lavoratori.

---

85 In merito, una parte della dottrina minoritaria ha proposto di ripensare l'oggetto del contratto di lavoro subordinato non tanto facendo riferimento alle mansioni dedotte in contratto quanto alla professionalità stessa del lavoratore. In tal senso Brollo M., *Tecnologie digitali e nuove professionalità*, in *Diritto delle Relazioni Industriali (DRI)*, n. 2, 2019, p. 478. Conformemente, altri autori sottolineano come "*l'incompletezza (*ndr. del contratto*) presuppone prassi e tecniche di determinazione progressiva delle condizioni convenute, riferite a una prestazione, meno fotografabile in termini di mansioni effettive, ma più di performance attesa, riferita ala capacità soggettive, immateriali e intellettuali in azione (…). In questo senso, per usare la terminologia del Codice civile, certamente determinabilità piuttosto che determinazione dell'oggetto*". Caruso B., *Strategie di flessibilità funzionale e di tutela dolo il Jobs Act: fordismo, post fordismo e industria 4.0*, in *Giornale di Diritto del Lavoro e di Relazioni Industriali (DLRI),* n. 1, 2018, p. 108.
86 In merito Pisani C., *Rapporto di lavoro e nuove tecnologie: le mansioni*, in *Giornale del Diritto del Lavoro e delle Relazioni Industriali (DLRI),* n. 2, 1988, p. 297.
87 Per *Data Mining* si intende una estrapolazione di dati in formato elettronico dalle innumerevoli fonti che compongono la rete Internet e i dispositivi ad essa connessi. Sul punto cfr. Stefano Neri, *La disciplina del Data Mining alla luce della proposta di regolamento comunitario in materia di trattamento di dati personali: criticità, limiti e prospettive de jure condendo*, in FiloDiritto, 20 aprile 2015, disponibile al sito: https://is.gd/P9YLmW.
88 Harrag F., *Text mining approach for knowledge extraction in Sahîh Al-Bukhari*, in *Computers in Human Behavior*, vol.30, 2014, pp. 558-566.
89 In merito si parla di *stress* lavoro-correlato. A riguardo cfr. Kim P.T., *Data-Driven Discrimination at Work*, in *William and Mary Law Review*, n. 58, 2017, pp. 857 ss.

Negli ultimi anni differenti studi di teoria dell'organizzazione hanno esplorato l'utilizzo di tecniche di *Data Mining* per la gestione delle risorse umane, conducendo *Sentiment Analysis* dei dipendenti per comprenderne atteggiamenti, percezioni e umori.
A tale riguardo gli esempi sono molteplici essendo stati analizzati, con algoritmi predittivi, dati acquisiti sui *social* dei dipendenti per identificare caratteristiche incompatibili con il ruolo svolto o prevedere conflitti[90].
Altri studi hanno rilevato gli stati d'animo valutando le espressioni facciali rilevate attraverso le telecamere presenti sul luogo di lavoro[91], oppure analizzando i toni di voce[92] al fine di aumentare la soddisfazione dei lavoratori.
È stata, inoltre, stimata la produttività dei dipendenti misurando movimenti, tono di voce, coesione e collaborazione tra colleghi attraverso l'utilizzo di sensori apposti sui *badge*[93]
Altre ricerche hanno interessato la condivisone delle conoscenze tra lavoratori di una stessa organizzazione acquisendo informazione dai *social*[94] o dalla rete *intranet* aziendale[95].
Infine, alcuni studi hanno condotto una vera e propria profilazione[96] dei lavoratori attraverso l'analisi dei movimenti corporei[97] o della postura, per identificare le emozioni dei soggetti osservati[98].
Le tecniche di *Sentiment Analysis* stanno, quindi, espandendo il proprio ambito di indagine grazie al maggior volume di dati acquisibili da fonti eterogenee, costituite dai sistemi digitali di gestione del personale o dagli applicativi per rendere la prestazione virtuale.
Le potenzialità di elaborazione dei sistemi algoritmici e di IA permettono, così, d'individuare modelli di correlazione in grado di definire aspetti che non sono inerenti ad ambiti propriamente professionali e che concernono aspetti più personali, quali possono essere un'opinione o un apprezzamento.

***

In forza delle potenzialità descritte, le tecniche di *Data Analysis* si stanno rapidamente diffondendo, potendo determinare l'efficienza, l'efficacia e l'impatto di un'organizzazione mediante analisi descrittive

---

90 Cfr. Punnoose R., Ajit P., *Prediction of employee turnover in organizations using machine learning algorithms*, in *International Journal of Advanced Research in Artificial Intelligence (IJARAI)*, vol. 5, n. 9, 2016, pp. 22 – 26; Robinson S. D., Sinar E., Winter J, *Social media as a tool for research: A turnover application using LinkedIn*, in *TIP: The Industrial-Organizational Psychologist*, vol. 52, n.1, 2014, pp. 133–141.

91 Subhashini R., Niveditha, P. R., *Analyzing and detecting employee's emotion for amelioration of organizations,* in *Procedia Computer Science*, n. *48*, 2015, pp. 530–536.

92 Chan C. F., Eric W. M., *An abnormal sound detection and classification system for surveillance applications*, in *Signal Processing Conference, 2010 18th European,* IEEE, August 2010, pp. 1851–1855.

93 Ara K., Akitomi T., Sato N., Tsuji, S., Hayakawa M., Wakisaka Y. et All, *Healthcare of an organization: Using wearable sensors and feedback system for energizing workers,* in *Proceedings of the 16th Asia and South Pacific Design Automation Conference ASPDAC,* IEEE, January 2011, pp. 567–572.

94 Van Zoonen W., Verhoeven J. W. M., Vliegenthart R., *How employees use Twitter to talk about work: A typology of work-related tweets,* in *Computers in Human Behavior*, n. 55, 2016, pp. 329–339.

95 Koriat, N., & Gelbard, R., *Knowledge sharing motivation among IT personnel: Integrated model and implications of employment contracts,* in *International Journal of Information Management*, vol. *34*, n. 5, 2014, pp. 577–591.
Koriat, N., & Gelbard, R., *Knowledge sharing analytics: The case of IT workers*, in *Journal of Computer Information Systems*, vol. 59, n. 4, 2017, pp. 1–11.

96 Art. 22 GDPR.

97 Preece S. J., Goulermas J. Y., Kenney L. P. J., Howard D., Meijer K., Crompton R., *Activity identification using body-mounted sensors—A review of classification techniques,* in *Physiological Measurement*, vol. 30, n. 4, 2009, R1–33.
Diego-Mas J. A., Alcaide-Marzal, J., *Using KinectTM sensor in observational methods for assessing postures at work*, in *Applied Ergonomics*, vol. 45, n. 4, 2014, pp. 976–985.

98 Rosário J. L., Diógenes M. S. B., Mattei R., Leite J. R., *Angry posture*, in *Journal of Bodywork and Movement Therapies*, n. 20(3), 2016, pp. 457–460.
Rosário J. L., Diógenes M. S. B., Mattei R., Leite J. R., *Differences and similarities in postural alterations caused by sadness and depression*, in *Journal of Bodywork and Movement Therapies*, vol. 18, n. 4, 2014, pp. 540–544.

(ossia che consentono di comprendere le prestazioni aziendali, presenti e passate, al fine di assumere decisioni informate), predittive (ovvero in grado di rilevare tendenze e di eseguire previsioni) e prescrittive (cioè che permettono di ottimizzare le prestazioni, rimodellando il processo decisionale)[99].
L'elaborazione dei dati può, per esempio, supportare l'organizzazione a rappresentare in maniera più inerente alla realtà i legami funzionali o gerarchici che tengono unite le persone all'interno dell'azienda.
L'analisi di dati può essere utilizzata, inoltre, per comprendere il *turnover* aziendale, identificando i motivi che spingono un soggetto (o un gruppo di individui) ad abbandonare o permanere all'interno di una realtà organizzativa.

Volendo esplicare come si concretizza il processo di *Data Analysis,* prendendo in considerazione il caso di valutazione del *turnover* aziendale l'indagine comporterà, in primo luogo, un'analisi descrittiva che valuti i dati storici dei lavoratori. In questo caso verranno analizzati, per esempio, dati afferenti al genere, all'età o ai profili di carriera per identificare le risposte corrispondenti alle caratteristiche di base del personale in forza.
L'algoritmo di analisi sarà tanto più performante, tanto maggiore sarà il *dataset* di analisi fornito. Tali informazioni potranno essere estrapolate da un singolo sistema (in genere HRIS) o da una combinazione dei dati acquisiti dai differenti sistemi (HRIS, CRM, *Digital Workplace*).
L'analisi descrittiva consente di compiere una diagnosi della situazione aziendale, finalizzata a comprendere quali fattori costituiscono elementi decisivi che inducono un dipendente a permanere presso l'azienda o a scegliere di variare impresa. In questo caso, si valuteranno gli stati di soddisfazione o insoddisfazione di un lavoratore, il proprio adattamento alla mansione e il grado di integrazione con l'organizzazione.
Successivamente, potranno essere elaborati dei modelli previsionali che consentono di ottenere delle informazioni prospettiche di quello che potrebbe accadere all'organico aziendale. In questa fase, i modelli prognostici vengono elaborati utilizzando dati storici e attuali.
Al termine delle fasi più propriamente "di studio", potranno essere elaborate le prescrizioni operative d'azione, ovvero le decisioni manageriali di gestione in base agli obiettivi che l'azienda si prefigge di ottenere.
Queste tre classi di elaborazione costituiscono una modalità di "analisi avanzata", venendo effettuate mediante strumenti sofisticati - autonomi o semiautonomi - che elaborano i dati, anche grezzi (ovvero non strutturati o non autoevidenti), in maniera da renderli utilizzabili e accessibili alle decisioni datoriali.
Tali tecniche includono complesse operazioni quale l'estrazione di testo, l'apprendimento automatico e la creazione di *pattern* di corrispondenza.
L'analisi mediante tecniche di *Data Analysis* consente, così, di ridurre i limiti quantitativi - insiti nell'operato umano - traendo conclusioni su dati eterogenei, anche di ingenti volumi.

L'acquisizione di dati è, quindi, la vera innovazione della gestione del lavoro, potendo ottenere dalla loro elaborazione – anche mediante sistemi anche di Intelligenza Artificiale (IA) - informazioni utili a fini decisionali.

[99] Cfr. Fabbri T., Scapolan A. C., *Digitalization and HR Analytics: a Big Game for an HR Manage*r, in *Human Resource Management and Digitalization*, Routledge/Giappichelli, 2018, pp. 243 – 254.

5. Gestione algoritmica dei lavoratori e tecniche utilizzate per compiere le analisi. In particolare: i sistemi di Intelligenza Artificiale (IA)

Quando si parla di "gestione algoritmica" o *Algorithmic Management*[100], dei lavoratori si intende fare riferimento a quella "*strumentazione informatica che non si limita a fornire misurazioni e valutazioni dei diversi aspetti dell'organizzazione, ma è in grado anche di formulare decisioni in autonomia senza l'intervento datoriale o manageriale"* ed è *"riconducibile all'Algorithmic Management"*[101].

La gestione algoritmica è, quindi, costituita dall'insieme di strumenti tecnologici e informatici che permettono la direzione a distanza del lavoro sulla base dei dati raccolti e utilizzati per delineare un processo decisionale automatizzato (o semiautomatico) rispondente agli obiettivi definiti dall'organizzazione.

L'utilizzo di tale accezione fa comunemente riferimento all'impiego di sistemi di Intelligenza Artificiale (IA), ovvero di quel settore dell'informatica in grado di elaborare sistemi che possono eseguire compiti normalmente svolti dall'intelligenza umana[102].

La sovrapposizione dei concetti di algoritmo e IA non è, però, del tutto corretta.

Con il termine algoritmo ci si riferisce a "*una sequenza finita di istruzioni ripetibili e non ambigue (…)*" che "*se eseguita con determinati dati in ingresso (input) produce all'uscita dei risultati (output) risolvendo una classe di problemi in un tempo finito*"[103].

Gli algoritmi costituiscono, quindi, una componente necessaria e insostituibile dei sistemi di IA e, se utilizzati per programmare, sono in grado di compiere ragionamenti deduttivi, induttivi e probabilistici[104].

L'espressione IA riguarda, invece, "*software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal*"[105].

La distinzione tra concetto di "algoritmo" e "Intelligenza Artificiale" è stata di recente elaborata anche dalla Terza sezione del Consiglio di Stato con la sentenza del 25 novembre 2021, n. 7891[106].

---

100 In merito Mateescu A., Nguyen A., *Algorithmic management in the workplace,* Data & Society Research Institute, February 2019; Adams-Prassl J., *What if Your Boss Was an Algorithm? Economic Incentives, Legal Challenges, and the Rise of Artificial Intelligence at Work*, in *Comparative Labor Law & Policy Journal 123*, vol. 41, n. 1, 2019, pp. 1 ss.; Aloisi A., De Stefano V., *Il tuo capo è un algoritmo. Contro il lavoro disumano,* Laterza, Bari, 2020, pp. 77-79; Ingrao A., *Data-Driven management e strategie di coinvolgimento collettivo dei lavoratori per la tutela della privacy,* in *Labour & Law Issues (LLI)*, n. 2, 2019 pp. 129-132; Gaudio G., *L'algorithmic management e il problema dell'opacità nel diritto oggi vigente e nella Proposta della Direttiva sul miglioramento delle condizioni dei lavoratori tramite piattaforma*, in *Lavoro Diritti Europa*, n. 1, 2022, pp. 1 ss.;

101 Ingrao A., Donini A., *Algoritmi e lavoro*, in *Labour Law Community* del 25 maggio 2022, p. 9, consultabile *online* https://www.labourlawcommunity.org/ricerca/algoritmi-e-lavoro/. Le autrici specificano che "*mentre le tecniche di analytics sono uno strumento di supporto per l'azione manageriale, l'algorithmic management comprende algoritmi sofisticati, che elaborano basi di dati più ampie o big data e, soprattutto, sono in grado di apprendere e costruire regole autonome che saranno poi applicate ad un determinato processo produttivo o ad una sua sezione*".

102 Cfr. Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *L'intelligenza artificiale per l'Europa*, Bruxelles, 25.4.2018 COM(2018) 237 final.

103 Sartor G., *L'informatica giuridica e le tecnologie dell'informazione. Corso d'informatica giuridica*, Terza edizione, Giappichelli, Torino, 2016, pp. 99 ss.

104 Cfr. Ingrao A, Donini A., *Algoritmi e lavoro*, in *Labour Law Community* del 25 maggio 2022, p. 3 consultabile *online* https://www.labourlawcommunity.org/ricerca/algoritmi-e-lavoro/.

105 The European Commission's High-Level Expert Group On Artificial Intelligence, *A definition of AI: main capabilities and scientific disciplines*, 18 December 2018, p. 7 (definizione che rielabora la definizione contenuta nella Comunicazione della Commissione europea, COM(2018)237, final).

106 Le definizioni di algoritmo e di Intelligenza Artificiale sono state formulate in occasione di un giudizio avente ad oggetto la legittimità di una procedura di gara per la fornitura di *Pacemaker* e Defibrillatori per gli enti sanitari lombardi. Per un approfondimento si rinvia a Cappellazzo N., *Algoritmi, automazione e meccanismi di intelligenza artificiale: la classificazione proposta dal Consiglio di Stato*, in *Federalismi.it* del 23 marzo 2022, pp. 1 ss.

Nella sentenza richiamata per "algoritmo" viene inteso una "*sequenza finita di istruzioni, ben definite e non ambigue, così da poter essere eseguite meccanicamente e tali da produrre un determinato risultato*», dall'altro lato è altrettanto vero che il concetto di algoritmo «*quando è applicato a sistemi tecnologici, è ineludibilmente collegata al concetto di automazione ossia a sistemi di azione e controllo idonei a ridurre l'intervento umano*".
Distintamente, il concetto di Intelligenza Artificiale fa riferimento a un algoritmo che "*contempla meccanismi di machine learning e crea un sistema che non si limita solo ad applicare le regole software e i parametri preimpostati (come fa invece l'algoritmo "tradizionale") ma, al contrario, elabora costantemente nuovi criteri di inferenza tra dati e assume decisioni efficienti sulla base di tali elaborazioni, secondo un processo di apprendimento automatico".*
Secondo i giudici del Consiglio di Stato, pertanto, mentre gli algoritmi possiedono una struttura predefinita, chiusa, rigida in quanto si compongono di una serie di passaggi individuabili *ex ante*, i sistemi di IA sono caratterizzati da tecniche di apprendimento automatizzato, come quelle di *Machine Learning*, le quali non limitano la macchina ad eseguire regole predeterminate, ma sono in grado di assumere decisioni efficienti sulla base di un processo di apprendimento autonomo. I sistemi di IA operano, quindi, in assenza di istruzioni preliminarmente esplicate da un operatore esterno.
Il concetto di "gestione algoritmica" deve, pertanto, essere interpretato in senso ampio, tale da ricomprendere non solo l'impiego di "algoritmi", in senso stretto, ma anche i sistemi di IA.

Quando si fa riferimento in maniera specifica all'Intelligenza Artificiale (IA)[107] si intende, quindi, una branca dell'informatica che si occupa di progettare sistemi che portino a termine attività cognitive che normalmente necessiterebbero dell'intelligenza umana, essendo in grado di auto-migliorarsi e auto-apprendere.
La disciplina nasce nel 1956 con il programma di Allen Newell e Herbert Simon, denominato *Logic Theorist*, che riproduceva un modello di ragionamento deduttivo. L'espressione "Intelligenza Artificiale" fu, però, introdotta successivamente dall'informatico John McCarthy[108].
I primi sistemi di IA mostravano *performance* inferiori rispetto a quelle ottenute da operatori umani e con risultati poco attendibili, in quanto soggetti a variabilità.
Oggigiorno, al contrario, le applicazioni dei sistemi di IA stanno dimostrando una capacità di elaborazione paragonabile a quella umana, portando a prospettare per il futuro un impiego dell'IA anche nell'ambito di ragionamenti cognitivi complessi.
Il concetto di IA è un termine ampio che racchiude al suo interno ulteriori sotto branche, di crescente complessità e autonomia, classificabili in riferimento alle differenti metodiche operative impiegate.

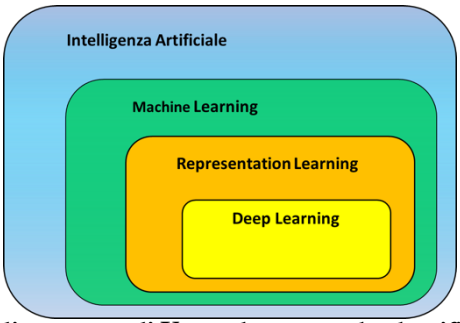


Figura 11: diagramma di Venn che mostra la classificazione dell'IA.

[107] Cfr. Gruppo indipendente di esperti ad alto livello sull'intelligenza artificiale, *Una definizione di IA: principali capacità e discipline*, Bruxelles, 2019. Anche nelle Proposte per una Strategia italiana per l'Intelligenza Artificiale, elaborate dal Gruppo di Esperti MISE e pubblicate dal Ministero dello Sviluppo Economico il 2 luglio 2020 (www.mise.gov.it), si individua con il termine IA "*una famiglia di tecnologie che spaziano dalla rappresentazione della conoscenza al ragionamento automatico che sottende aree quali la pianificazione e il supporto decisionale, fino alla percezione e all'apprendimento automatico*".
[108] Per una ricostruzione sullo sviluppo dei sistemi di IA cfr. Portinale L., *Intelligenza Artificiale: storia, progressi e sviluppi tra speranze e timori*, in *Media Laws*, n. 3, 2021, pp. 13- 28.

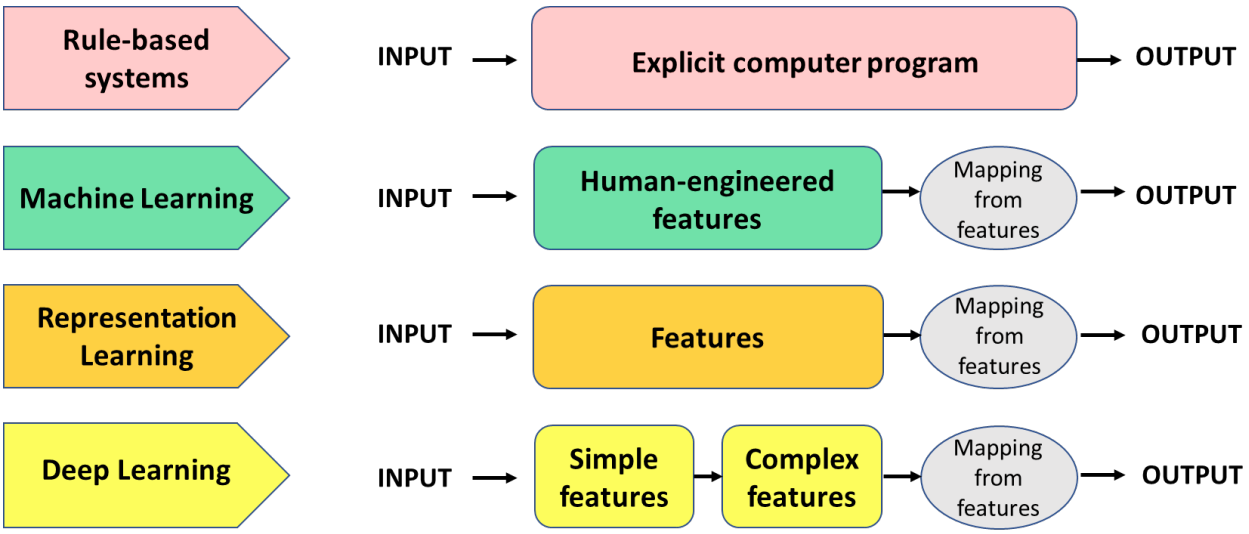


Figura 12: schema in cui si confrontano sistemi basati su una programmazione esplicita fornita dall'uomo (in rosa) e tre sistemi di IA (in basso, evidenziati in verde, arancio e giallo).

Il primo metodo di IA è *Machine Learning* (ML)[109], una tecnica in cui i programmi vengono "allenati" a eseguire compiti senza una programmazione informatica esplicita sottostante, ma rilevando *pattern* in modo automatico direttamente dai dati forniti.
Il *Machine Learning* è, quindi, un "*tipo specifico di intelligenza artificiale che consiste in un processo automatico di individuazione di correlazioni tra variabili all'interno di un set di dati, allo scopo di compiere previsioni o stime di certi effetti. In sostanza, ai sistemi di machine learning – o di apprendimento automatico – viene assegnato un obiettivo e fornita una vasta mole di dati da utilizzare come esempi del modo in cui l'obiettivo può essere raggiunto o dai quali far derivare modelli di decisione. Il sistema, analizzando i dati forniti, "impara" come meglio realizzare l'obiettivo richiesto*"[110].
Il programma è, dunque, in grado di imparare analizzando i dati forniti ed effettuare previsioni quando vengono inseriti nuovi dati.
Il problema principale di tale tecnica è però quello che, per analisi complesse, può non essere chiaro al programmatore stabilire a priori quali caratteristiche l'algoritmo deve selezionare.

Il *Representation Learning* (*RL*) costituisce una sottoclasse del ML. In questo caso è il programma che impara autonomamente a scegliere le caratteristiche migliori per classificare i dati forniti in *input*.
Un sistema di *RL*, sottoposto a un *training* adeguato (ovvero capace di fornire abbastanza esempi per "allenarlo"), può classificare le informazioni introdotte in maniera più performante rispetto un sistema di *ML*, in cui le proprietà di analisi sono selezionate da un operatore umano.

Il *Deep Learning* (DL) è un tipo di RL caratterizzato dall'utilizzo di reti neurali "multistrato".
In questo caso, il programma ricava autonomamente un insieme di proprietà che rispecchiano l'organizzazione gerarchica dei dati posti a *input*.

---

[109] Cfr. Royal Society (UK), *Machine learning: the power and promise of computers that learn by example* (April 2017), p.19.
[110] Zuddas P., *Intelligenza Artificiale e discriminazioni,* in Consulta online, 16 marzo 2020, p. 1. Un'ulteriore definizione ci viene fornita da Lombardi e Macchi per i quali i sistemi di *Machine Learning* sono "un insieme di metodi (algoritmi + programmi) in base ai quali si cerca di ottimizzare una prestazione alla luce dei dati e dell'esperienza passata" capaci di esprimere una "intelligenza computazionale". Lombardi M., Macchi M., *Il lavoro tra intelligenza artificiale e intelligenza umana*, in Cipriani A., Gramolati A., Mari A. (a cura di), *La Quarta Rivoluzione industriale e le trasformazioni delle attività lavorative*, Firenze University Press, 2018, p. 304, disponibile *online*.

Con il DL le rappresentazioni complesse sono interpretate[111] come l'unione di raffigurazioni più semplici, senza necessità di definire a priori quali caratteristiche analizzare.
Per fare ciò, il DL opera mediante una rete neurale artificiale[112] costituita da una serie di nodi.
Ognuno di questi "neuroni artificiali" è in grado di compiere azioni elementari, come ricevere informazioni dai nodi limitrofi e inviare risposte a tutti gli elementi connessi.
I nodi, dopo la ricezione di *input,* sotto forma di valori, valutano le "proprietà" dei dati acquisiti individuando il "peso" corrispondente per ognuno.
Successivamente, ciascun "neurone artificiale" produce una "decisione" in ragione della "pesatura" compiuta.
L'informazione in ingresso, mediante l'elaborazione operata dalle connessioni neuronali, diviene dato in uscita ovvero un *output*.
Una rete neurale opera, quindi, sovrapponendo nodi organizzati in strati (definiti *layers*) che agiscono in sequenza: gli *output* dei nodi precedenti diventano gli *input* di quelli successivi.
Proprio l'architettura "multistrato", di cui è composta la rete neurale, ha ispirato il nome "*Deep Learning*", ovvero "apprendimento profondo".

Il primo strato è composto delle unità di *input* che acquisiscono dati dall'esterno e li trasmettono all'interno della rete neurale. I dati ricevuti vengono processati e trasformati in informazioni che vengono comunicate allo strato delle unità nascoste (o *hidden)*. Lo strato *hidden* elabora le informazioni ricevute mediante le singole unità, fino ad arrivare all'*output*.

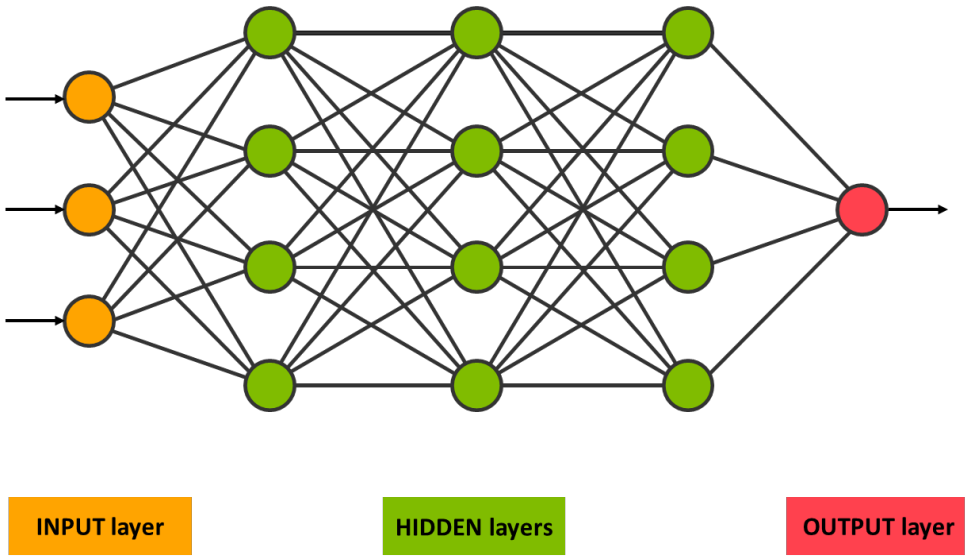


Figura 13: schema raffigurante il concetto di rete neurale costituita da nodi (neuroni artificiali) interconnessi tra loro; in questo esempio vi sono tre nodi di input, tre strati nascosti ognuno formato da quattro nodi e uno strato di output costituito da un solo nodo.

[111] IA intesa, dunque, come un processo analitico iterativo, che permette al sistema di progredire, generare in un ciclo continuo nuovi modelli sulla base dei dati di feedback, così da adeguare, modificare, perfezionare in modo autonomo le proprie azioni, in termini non sempre prevedibili, ma sempre funzionali. In merito Peruzzi M., *Il diritto antidiscriminatorio al test di intelligenza artificiale*, in *Labour & Law Issues (LLI),* vol. 7, n. 1, 2021, p. I 56; Comandè G., *Intelligenza artificiale e responsabilità tra* liability *e* accountability. *Il carattere trasformativo dell'IA e il problema della responsabilità*, in *Analisi giuridica dell'economia*, n. 1, 2019, pp. 172 ss.
[112] Sanguinetti G., *Machine Learning: accuratezza, interpretabilità e incertezza*, *Ithaca: Viaggio nella Scienza*, n. 16, 2020, p. 74; Ruffolo U., *Intelligenza artificiale, machine learning e responsabilità da algoritmo*, in *Giurisprudenza Italiana*, n. 7, 2019, pp. 1657 ss; Portinale L., *Intelligenza Artificiale: storia, progressi e sviluppi tra speranze e timori*, in *Media Laws*, n. 3, 2021, p.15.

***

Contestualizzando il processo di una rete neurale in riferimento alle analisi che possono interessare la gestione del personale, il primo strato (*input layer)* potrebbe essere costituito dalle interazioni compiute dai lavoratori all'interno di una *Digital Workplace*.
Gli strati intermedi (*hidden layers)*, ovvero quelli che forniscono una rappresentazione interposta nel processo di analisi, compierebbero la "pesatura" dei valori introdotti.
Nel caso di specie, i singoli "*click*" compiuti dai lavoratori sulla piattaforma verrebbero "pesati" in riferimento ad ogni attività svolta nell'ambiente digitale (come accedere a documenti *word* oppure inviare comunicazione a colleghi mediante la rete *intranet*).
Nella fase intermedia avviene la vera e propria "elaborazione" posta a individuare le correlazioni tra i dati immessi.
L'*output layer*, a conclusione del processo di analisi, fornirebbe i risultati dell'elaborazione attraverso una classificazione o categorizzazione dei valori, immessi come *input,* in riferimento ai *pattern* di correlazione individuati.
L'esito del processo potrebbe, per esempio, individuare il numero di interazioni tenute dal lavoratore con determinati colleghi oppure la frequenza di accesso agli applicativi di redazione documenti.

6. Nuove tecnologie e potere di controllo direttivo

L'introduzione delle tecnologie ICT ha apportato un cambio di paradigma nel controllo dei lavoratori orientato ad un'analisi, talvolta completamente automatica, dei dati.
Il potere di controllo si tramuta in controllo dei dati[113] divenendo la "porta d'accesso" preferenziale per acquisire informazioni sui prestatori spendibili non solo per monitorare, ma anche per gestire i rapporti di lavoro.
Il controllo esercitato mediante gli strumenti digitali costituisce una fonte potenzialmente inesauribile di informazioni, specialmente se ottenute a seguito dell'elaborazione di dati "grezzi".
Nel processo di controllo tecnologico vi è una costante: l'utilizzo di dati (sempre più spesso "non autoevidenti") e il necessario intervento di una fase intermedia, spesso interamente automatizzata, per poter comprendere il significato delle informazioni.
Tra acquisizione e utilizzo dei dati vi è, quindi, un momento di elaborazione capace di "tradurne" il significato e idoneo a disvelare nuove informazioni prima non comprensibili.
La diffusione delle tecniche di *Data Analysis* influenza, conseguentemente, l'intensità del controllo datoriale divenuto sempre più sofisticato attraverso una gestione *Data Driven.*
Il potere di controllo si rafforza dotandosi di nuove abilità: ciò non solo in ragione degli strumenti innovativi impiegati, ma anche per la tipologia di dati acquisibili.
Quest'ultimi, infatti, possono essere caratterizzati da una "non autoevidenza" da cui la necessità di una fase di elaborazione che li renda intellegibili. Operazione che pone il datore di lavoro nella condizione di accedere a nuove informazioni sui lavoratori.

[113] Definito anche come *Big Data Analytics* in ragione dell'eterogeneità e dei grandi volumi delle informazioni fornite dai dispositivi digitali impiegati. In merito Rota A., *Rapporto di lavoro e big data analytics: profili critici e risposte possibili*, in *Labour & Law Issues (LLI)*, 2017, vol. 3, n. 1, pp. I34 ss; Dagnino, E., *People analytics: lavoro e tutele al tempo del management tramite big data*, in *Labour & Law Issues (LLI)*, vol. 3, n. 1, pp. R37 ss., Dessì O., *Il Controllo a distanza sui lavoratori. Il nuovo art. 4 Stat. lav.*, Edizioni scientifiche italiane, Napoli, 2017 pp. 181-185; Stizia A., Lopez B., *Le più avanzate modalità di controllo sul lavoratore: machine learning e social media*, in Pisani C., Proia G., Topo A. (a cura di) *Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro*, Giuffrè Editore, Milano, 2022, pp. 358 ss.

Le potenzialità afferenti ai dispositivi diffusi dalla quarta rivoluzione industriale ci pongono, così, di fronte a un "gemello" della fisicità, un *Digital Twin*[114]*,* oggetto di monitoraggio e nuovo elemento delle dinamiche organizzative.
La tecnologia consente, quindi, un controllo prima non possibile, capace di dedurre specifiche caratteristiche professionali e personali sulla base di dati non immediatamente correlati alle stesse.
In altre parole, anche senza richiedere dirette informazioni sull'eventuale appartenenza sindacale di un lavoratore, questa può essere desunta dalle elaborazioni algoritmiche impostate sui dati acquisiti.
Parimenti, anche la religione o l'origine etnica di un soggetto potrebbero essere determinate a seguito di un processo di *Data Analysis,* correlando statisticamente il codice postale o il domicilio di residenza[115].
Conseguentemente, assumere una decisione inerente a un lavoratore fondandola sull'ubicazione dell'alloggio potrebbe celare una disposizione basata su caratteristiche personali.

Anche l'esercizio del potere direttivo appare influenzato dall'innovazione digitale e orientato, nelle imprese che adottano tali meccanismi, a raccogliere quante più informazioni possibili sui lavoratori, necessarie per elaborare le "migliori" decisioni algoritmiche[116].

Per la parte datoriale è diventato, così, sempre più rilevante acquisire grandi volumi di dati, al fine di sviluppare una conoscenza approfondita delle capacità e attitudini dei propri dipendenti. Informazioni che delineano l'identità di un "gemello digitale" su cui poggiare le nuove architetture organizzative.
Allo stesso modo in cui un'azienda approfondisce la conoscenza sui propri clienti (si veda la diffusione dei sistemi *CRM*), così i datori di lavoro cercano di recepire quante più notizie possibili sui loro dipendenti (anche potenziali) per comprendere se questi saranno adatti al ruolo assegnato, se potranno raggiungere gli obiettivi prefissati o se si adatteranno all'ambiente aziendale, anche da un punto di vista relazionale.

Il denominatore comune delle nuove tecnologie per il controllo e la gestione dei lavoratori è, quindi, la raccolta di dati e la loro elaborazione.
Attività che, a dire il vero, è sempre stata compiuta nell'ambito dei rapporti di lavoro, ma vincolata al limite naturare "dell'utilizzabilità dei dati" rimesso alle capacità umana di analisi.
Le nuove tecnologie intervengono su tale processo e, grazie alla diffusione della *Data Analysis*, avviene una facilitazione nell'interpretazione.
Per tale ragione, l'impiego di dispositivi supportati da sistemi algoritmici o di IA risulta già diffusa in un'ampia gamma di attività riguardanti il rapporto di lavoro[117]: dalle assunzioni al controllo delle attività.
L'uso della tecnologia per osservare i lavoratori ha, quindi, mutato radicalmente la natura delle fonti e le modalità di acquisizione dei dati, nonché il modo di trattarli, soprattutto a fini decisionali.

---

114 In merito Faioli M., *Data Analytics, robot intelligenti e regolazione del lavoro*, in Focus lavoro, persona, tecnologia del 23 marzo 2022 su *Federalismi.it*., p.153 il quale osserva che "*quel gemello, già oggi, interagisce attivamente con l'essere umano e con gli strumenti che si usano per produrre e erogare servizi, creando una connessione continua tra ciò che accade nella realtà e ciò che digitalmente può essere elaborato per migliorare la realtà in cui siamo immersi. Nel tempo, quel gemello digitale potrà svolgere, con e al posto dell'essere umano, ciò che normalmente si ritiene debba essere realizzato dalla persona*". Sul *Digital Twin* anche il recente rapporto di Confindustria Digitale Anitec-Assinform 2021 pubblicato sul sito di Anitec-Assinform e gli studi di Roberto Saracco sul sito IEEE Future Dirctions.
115 Crf. Corte giust. 16 luglio 2015, C- 83/14, *Chez Razpredelenie Bulgaria AD* contro *Komisia za zashtita ot diskriminatsia* sulla discriminazione associata. Per un approfondimento si rinvia al capitolo 3.
116 Attinenti, per esempio, all'attribuzione di premi, alla distribuzione dell'orario di lavoro o al riconoscimento di promozioni.
117 In prospettiva, questi strumenti digitali saranno "*sempre più usati per prendere decisioni che finora sono state parte essenziale delle responsabilità manageriali di gestione dei rapporti di lavoro",* Treu T.*, La digitalizzazione del lavoro: proposte europee e piste di ricerca,* in *Federalismi.it,* n.9, 2022, p. 201.

Dispositivi come HRIS*, Digital Workplace,* CRM*,* AST stanno incrementando il volume di dati disponibili, trattandosi di apparecchiature caratterizzate da un'intrinseca commistione tra le capacità di registrare e archiviare informazioni, oltre che di elaborarle.
Il diffondersi di questi strumenti ha, quindi, "*accelerato tendenze già in atto nelle trasformazioni delle strutture sia del lavoro sia delle imprese con conseguenze ancora largamente indeterminate*"[118].

La digitalizzazione sembra, così, consentire l'esercizio sincrono del potere di controllo e direttivo, sino a contaminare il primo facendogli assumere le sembianze di un nuovo "potere di controllo direttivo"**[119].**
L'esercizio del potere di controllo datoriale costituisce, dunque, il mezzo attraverso cui accedere ad un ampio volume di informazioni sui lavoratori.
In forza di ciò, il potere di controllo si abilita di nuove capacità modificando la propria natura e travalicando la tradizionale divisione tra poteri datoriali.
Nei contesti organizzativi ad alto contenuto tecnologico, ove il virtuale si sostituisce al reale, il potere di controllo giunge a confondersi con il potere direttivo, dando forma a una "originale" manifestazione di autorità datoriale.
Acquisire dati grezzi "non autoevidenti" per finalità di controllo ed elaborarli, per comprenderne il valore, pone il datore di lavoro in una condizione di "supremazia informativa" valida non solo a monitorare, ma anche a prendere decisioni.
Il controllo tecnologico diviene, così, il punto d'accesso principale alle informazioni, consentendo al datore di lavoro di esercitare in maniera inedita i propri poteri.
Il "potere di controllo direttivo" evidenzia, quindi, come il controllo dato dalla tecnologia rappresenti la manifestazione del cambiamento, divenendo sempre più sfumata la linea di confine tra controllo dell'attività lavorativa e monitoraggio compiuto per esigenze imprenditoriali[120].
Per esempio, l'analisi di dati grezzi al fine di mettere in risalto la *performance* dei singoli lavoratori, può generare una capillare consapevolezza di come viene eseguita l'attività lavorativa con una fusione (quasi) totale del potere di controllo e direttivo.
Il potere datoriale si dilata, per effetto delle tecnologie abilitanti, dando forma ad una manifestazione di potere ibrida e sofisticata: sia per la capacità di elaborare dati "non autoevidenti" - da cui trarre nuove informazioni - sia per le potenzialità decisionali rimesse al datore di lavoro.
Si realizza, in tal modo, un'accentuazione dell'asimmetria funzionale a discapito della parte debole del rapporto, ovvero i lavoratori.

Si delinea, così, una nuova soglia di criticità.
Il controllo è la causa e la (diretta) conseguenza dell'analisi dei dati e anche ove non sia "*l'obiettivo primario del datore di lavoro che ricorre alle tecnologie*, *(…) ne costituisce un'inevitabile conseguenza dell'utilizzo delle medesime*"[121].

---

[118] Treu T.*, La digitalizzazione del lavoro: proposte europee e piste di ricerca,* in *Federalismi.it*, n.9, 2022, p. 193.
[119] Cfr. Tebano L., *Lavoro, potere direttivo e trasformazioni organizzative*, Editoriale Scientifica, Napoli, 2020, pp. 239 – 252; Tebano L, *Fabbrica 4.0 e potere di "controllo direttivo"*, in Rusciano M., Gaeta L., Zoppoli L. (a cura di), *Mezzo secolo dallo statuto dei lavoratori*, in *Quaderni della Rivista Diritti Lavori Mercanti, n. 8, 2020, pp.,* 443 ss.; Tebano L*., La digitalizzazione del lavoro tra intelligenza artificiale e gestione algoritmica*, in *LANUS*, n. 24, 2021, pp. 43 ss.
[120] Tale interpretazione si avvicina alla prospettiva aziendalista post-moderna ove il potere di controllo rappresenta, in primo luogo, la manifestazione del cambiamento organizzativo. Secondo tale rappresentazione, i controlli si rivelano funzionali a orientare i comportamenti e ad allinearli alle caratteristiche del contesto i n cui la prestazione viene resa. In merito Tebano L., *Lavoro, potere direttivo e trasformazioni organizzative*, Editoriale Scientifica, Napoli, 2020, p. 242; Spincer A., Alvesson M., Karreman D., *Resisting resistance. Critical performativity. The unfinished business of critical management studies*, in *Human Relations*, vol. 62, n. 4, 2009, pp. 537 ss.
[121] Dessì O., *Il Controllo a distanza sui lavoratori. Il nuovo art. 4 Stat. lav*., Edizioni Scientifiche Italiane, Napoli, 2017, p. 183.

Gli innovativi strumenti lavorativi permettono di elaborare informazioni apparentemente "neutre", ma capaci di definire un profilo completo del lavoratore non solo da un punto di vista strettamente professionale.
Informazioni che possono essere impiegate per controllare, ma anche per organizzare il rapporto di lavoro rendendo sempre più sfumato il confine tra osservabilità, controllo e gestione.
Le potenzialità rimesse dalla tecnologia ai poteri datoriali possono, così, determinare l'insorgere di rischi per i diritti e le libertà dei lavoratori, osservati scrupolosamente e descritti sulla base di modelli di correlazione in grado di definire aspetti personali.
Le potenzialità di elaborazione dei sistemi algoritmici e di IA permettono, così, di attuare un trattamento suscettibile di cagionare un danno fisico, materiale o immateriale[122].
Un'elaborazione di dati personali che sia in grado di fornire una rappresentazione, ancorché sintetica, di un individuo ha inevitabilmente un impatto sui diritti della personalità[123].
La manifestazione del nuovo "potere di controllo direttivo" può, dunque, determinare la contestuale lesione della dignità e dell'identità personale consentendo che venga espletato un controllo vessatorio abilitato a conoscere non solo ogni attività lavorativa compiuta, ma volto anche a decifrare elementi ulteriori che travalicano l'ambito della mera professionalità.
La raffigurazione dei lavoratori realizzata con l'analisi dei dati può, quindi, alterare la conoscenza delle caratteristiche professionali note al datore di lavoro e porre nella disponibilità di quest'ultimo informazioni afferenti alla sfera personale.
In tal modo, i lavoratori rischiano di essere privati dei loro diritti fondamentali[124] subendo trattamenti discriminatori o perdendo il controllo effettivo dei propri dati personali.
Le tecniche avanzate di analisi dei dati possono, infatti, ledere la *privacy* violando la libertà di auto-determinazione informativa[125] degli interessati.
I processi di analisi e correlazione, in particolar modo se automatizzati, rischiano così di tradursi in trattamenti non trasparenti con il pericolo di utilizzare le informazioni acquisite in maniera difforme alle finalità preventivamente individuate.
La manipolazione dei dati può, quindi, impattare anche sull'equilibrio vita-lavoro proprio a causa dei confini sempre più sfumati tra ambito professionale e personale.
Il controllo tecnologico può, infine, raggiungere livelli di autonomia tali da far venire meno il diritto alla sorveglianza umana, ovvero il diritto dei prestatori a non essere gestiti e giudicati esclusivamente da una macchina.
Elaborare e correlale dati consente, quindi, di ottenere un'interazione più articolata con i lavoratori facendo emergere inferenze non prevedibili e informazioni non ricercate, in quanto ignote *ex ante*.
L'ampiezza di potere acquisita dal "controllo direttivo" e la corrispondente crescita dei rischi alla dignità e riservatezza in cui possono incorrere i prestatori comporta la necessità di (ri)definire i limiti entro cui questo si può manifestare.

In tale scenario, il quadro regolativo esistente potrebbe non risultare sufficiente ad evitare lesioni ai diritti dei lavoratori.

---

122 Cfr. Considerando 75 del GDPR.
123 Cfr. Donini A., *Tecniche avanzate di analisi dei dati e protezione dei lavoratori*, in *Diritto delle Relazioni Industriali (DRI)*, n.1/XXVIII, 2018, p. 226.
124 Cfr. Tullini P., *Economia digitale e lavoro non standard*, in *Labour & Law Issues (LLI)*, n. 2, 2016, p. 6.
125 Cfr. Donini A., *Tecniche avanzate di analisi dei dati e protezione dei lavoratori*, in *Diritto delle Relazioni Industriali (DRI)*, n.1/XXVIII, 2018, p. 226.

L'importanza di queste trasformazioni è riflessa nelle preoccupazioni e negli interrogativi delle istituzioni nazionali e internazionali[126].

Anche le Parti sociali europee hanno iniziato a confrontarsi sul tema della digitalizzazione e dell'Intelligenza Artificiale ritenendo che il rapido sviluppo della tecnologia e il suo impatto sulla vita dei lavoratori debba essere regolato congiuntamente con strumenti normativi e di dialogo sociale[127].

Per tale ragione, appare opportuno indagare su come la categoria del controllo datoriale si rapporti alle potenzialità di elaborazione di cui sono dotate le nuove tecnologie in relazione alle distinte categorie di dati acquisibili. In particolare, ci si domanda come il rinnovato "potere di controllo direttivo" interagisca con la categoria di dati "non autoevidenti".

È mediante l'interpretazione dei dati che può, infatti, pienamente manifestarsi il controllo nella nuova espressione di potere ibrido.

Il "potere di controllo direttivo" deve, quindi, trovare un assetto nel proprio esercizio che consenta di bilanciare i rischi, in cui possono incorrere i lavoratori, con gli interessi datoriali.

La ponderazione tra le distinte prerogative conduce a ricercare una proporzione che permetta lo sviluppo delle nuove manifestazioni del lavoro digitale tutelando i lavoratori dai pericoli insiti alle tecnologie.

Lo studio, quindi, di un "rischio proporzionato"[128] al fine di proteggere i diritti dei prestatori senza ostacolare eccessivamente l'attività imprenditoriale.

La valutazione delle possibili minacce richiede un approccio analitico innovativo e differente da quello impiegato per analizzare i pericoli efferenti alle prestazioni "analogiche".

La digitalizzazione della prestazione e l'impiego di sistemi di elaborazione dei dati influenza, infatti, *"non solo le modalità, ma la logica stessa della gestione dei rapporti di lavoro*"[129].

Comprendere, quindi, come si sviluppi l'istituto del controllo, analizzando le potenzialità a cui è abilitato e confrontando tale inedita manifestazione di autorità datoriale ai limiti vigenti, è un processo finalizzato a capire se i lavoratori digitali ricevano.

---

126 Una attenzione particolare è riservata all'impatto delle piattaforme digitali che intermediano o gestiscono il lavoro, In merito Commissione Europea, *Digitalization in the workplace, Eurofound*, novembre 2021; International Labour Organization, *Rapporto* ILO, 2021, *Work employment and social outlook 2021. The role of digital labour platforms in transforming the world of work*, Geneva; Treu *T., La digitalizzazione del lavoro: proposte europee e piste di ricerca,* in *Federalismi.it,* n.9, 2022, pp. 190- 211; Wood A., *Algorithmic management Consequences for Work Organisation and Working Conditions*, in *JRC Working Papers Series on Labour*, *Education and Technology*, n. 7, 2021, pp. 1 ss.

127 In questa luce va intesa l'adozione dell'Accordo quadro europeo sulla digitalizzazione del 22 giugno 2020 dalle parti sociali intersettoriali europee e applicato a tutta l'UE/SEE che mira a realizzare una positiva integrazione delle tecnologie digitali sul posto di lavoro prevenendo e minimizzando i rischi per lavoratori e datori di lavoro. l'Accordo quadro europeo rileva quattro sfide connesse allo sviluppo della digitalizzazione. La prima sfida è denominata *"Competenze digitali e sicurezza dell'occupazione"* e affronta l'effetto dirompente della digitalizzazione con riferimento alla continua obsolescenza di alcuni lavori, processi o competenze tradizionali. La seconda questione si riferisce alle modalità di connessione e disconnessione dei lavoratori durante la loro attività lavorativa. La terza sfida fa riferimento all'Intelligenza Artificiale (AI) e alla necessità di garantire e salvaguardare il principio "*human in control*", ovvero la scelta umana su come e se delegare le decisioni a un sistema automatizzato. L'ultima sfida affrontata dall'EFAD è strettamente connessa alla precedente. Riguarda la necessità di garantire il rispetto della dignità umana, minimizzando i rischi per un uso non trasparente dei dati. In merito Senatori I., *The European Framework Agreement on Digitalisation: a Whiter Shade of Pale,* in *Italian Labour Law e Journal,* vol. 13, n. 2, 2021, pp. 159-175; Rota A., *Sull'Accordo Quadro europeo in tema di digitalizzazione del lavoro,* in *Labor & Law Issues (LLI),* vol. 6, n. 2, 2020, pp. C.23-C.48.

128 Il concetto di "rischio proporzionato" la si rinviene anche Proposta di Regolamento sull'IA che si prefigge di garantire "*un approccio normativo orizzontale all'IA equilibrato e proporzionato, che si limita ai requisiti minimi necessari per affrontare i rischi e i problemi ad essa collegati, senza limitare od ostacolare indebitamente lo sviluppo tecnologico o altrimenti aumentare in modo sproporzionato il costo dell'immissione sul mercato di soluzioni di IA*" (p.3).

129 Treu T.*, La digitalizzazione del lavoro: proposte europee e piste di ricerca,* in *Federalismi.it,* n.9, 2022, p. 201.

Capitolo 2
Nuove tecnologie e potere di controllo

Parte 1
La disciplina del controllo a distanza

1.1. Nuove tecnologie e potere di controllo: dalla digitalizzazione alla datificazione del lavoro

Uno dei fattori che ha avuto il maggior impatto sui rapporti di lavoro è l'introduzione di nuove tecnologie dell'informazione e comunicazione (ICT) proprie dell'Industria 4.0.

Come si ha avuto modo di illustrare nel capitolo precedente, la digitalizzazione degli spazi di lavoro e la connessione degli strumenti per la gestione del personale (abilitati al *web* e predisposti a una centralizzazione delle informazioni) ha profondamente modificato il *management* e l'organizzazione dei lavoratori grazie al fenomeno della datificazione.

A tale riguardo, sono anche stati coniati nuovi termini quali *Algorithmic Management*[130] o *Data Driven Management*[131], volti a definire quei processi manageriali che delegano a strumenti algoritmici o di Intelligenza Artificiale il compito di assumere decisioni nei confronti dei lavoratori sulla base dei dati acquisiti.

Con tali sistemi i dati raccolti sono analizzati tramite algoritmi (in senso lato[132]) al fine di trarne informazioni nuove e rilevanti, quali tendenze o modelli predittivi, utili a implementare l'efficienza dei procedimenti organizzativi tradizionali o ad innovare l'offerta dei servizi.

La gestione algoritmica è, quindi, costituita dall'insieme di strumenti tecnologici che permettono la direzione a distanza del lavoro sulla base dei dati raccolti e impiegati per delineare un processo decisionale automatizzato (o semiautomatico) sulla base degli obiettivi definiti dall'organizzazione.

La nuova tecnologia muta, così, profondamente il rapporto di lavoro.

In primo luogo, consentendo di traslare l'attività lavorativa in una "dimensione digitale", svincolando la prestazione dalle coordinate spazio-temporali e consentendone l'esecuzione in ogni luogo e tempo.

Contestualmente, varia l'oggetto dell'osservazione.

La digitalizzazione del lavoro, datificando l'attività lavorativa, offre nuovi *output* su cui esercitare le prerogative datoriali, ovvero i dati. Questi, una volta acquisti, possono essere analizzati, elaborati e correlati per differenti esigenze.

Le nuove tecnologie applicate al lavoro portano, inoltre, ad un progressivo sovrapporsi sino a determinare la strutturale coesistenza degli strumenti di lavoro e di controllo, abilitati ad osservare non solo le immagini o le voci dei lavoratori, ma anche i dati ovvero le "tracce digitali" dei dipendenti.

Il problema del controllo a distanza si pone, così, laddove le capacità di analisi delle informazioni delineano situazioni di controllo (potenzialmente) diretto o sproporzionato.

---

130 In merito Mateescu A., Nguyen A., *Algorithmic management in the workplace,* in *Data & Society Research Institute*, February 2019; Adams-Prassl J., *What if Your Boss Was an Algorithm? Economic Incentives, Legal Challenges, and the Rise of Artificial Intelligence at Work*, in *Comparative Labor Law & Policy Journal 123*, vol. 41, n. 1, 2019, pp. 1 ss.; Aloisi A., De Stefano V., *Il tuo capo è un algoritmo. Contro il lavoro disumano,* Laterza, Bari, 2020, pp. 77-79; Ingrao A., *Data-Driven management e strategie di coinvolgimento collettivo dei lavoratori per la tutela della privacy,* in *Labour & Law Issues (LLI)*, n. 2, 2019 pp. 129-132; Gaudio G., *L'algorithmic management e il problema dell'opacità nel diritto oggi vigente e nella Proposta della Direttiva sul miglioramento delle condizioni dei lavoratori tramite piattaforma*, in *Lavoro Diritti Europa*, n. 1, 2022, pp. 1 ss.

131 In tema si veda il Rapporto OECD, *Data-Driven Innovation. Big Data for Growth and Well-Being,* 2015.

132 In merito si rinvia al capitolo 1 punto 5.

Si deve, infatti, tenere in considerazione che acquisire ingenti volumi di dati non comporta possedere un pari numero di informazioni utilmente spendibili: i dati acquisiti non sono sempre immediatamente comprensibili.
La maggior parte degli *output* prodotti dalle tecnologie ICT, infatti, non possono essere definiti come "autoevidenti", ma necessitano di un passaggio intermedio interpretativo.
Ciò introduce una nuova fase nell'esercizio del potere direttivo, ovvero quella dell'elaborazione dei dati, che porta a far riflettere sulle modalità in cui può essere esercitato il controllo a distanza.
Quando nel 1970 il Legislatore ha disciplinato i controlli mediante "apparecchi", ne ha descritto i limiti riferendosi a un monitoraggio compiuto su attività analogiche con strumenti ultronei rispetto quelli utilizzati dai dipendenti per rendere la prestazione.
I dispositivi di controllo erano, dunque, non essenziali all'attività lavorativa e (soprattutto) fornivano un'osservazione "autoevidente", ovvero di per sé stessa significativa senza necessità di alcuna elaborazione dei dati acquisiti.
Diversamente, strumenti tecnologici per l'esecuzione di prestazioni "native digitali" integrano in maniera inscindibile le capacità di lavoro con le potenzialità di controllo, offrendo un'osservazione illimitata delle attività compiute dai lavoratori negli ambienti virtuali.
Tale monitoraggio non è, però, sempre comprensibile dato che i dati acquisiti risultano per la maggior parte "non autoevidenti".

Per tale motivo, la digitalizzazione e la datificazione del lavoro e la conseguente elaborazione dei dati "non autoevidenti", devono indurre il Legislatore, da un lato, e l'interprete, dall'altro, a valutare le tutele esistenti al fine di vagliare la validità delle medesime in riferimento alle nuove potenzialità introdotte dalla tecnologia.
Ciò al fine di definire un sistema di protezione adeguato alle nuove esigenze "interpretative" che riesca a garantire un impiego legittimo e proporzionale dei dati (acquisiti o disvelati).
Le prerogative datoriali devono, infatti, essere bilanciate alle esigenze di dignità e riservatezza dei lavoratori affinché il controllo non divenga vessatorio e il trattamento dati illecito.
L'istallazione di strumenti digitali per il controllo dovrebbe, infatti, impedire l'acquisizione di informazioni estranee alla sfera lavorativa del lavoratore o eccedenti rispetto alle finalità di trattamento individuate.
Valutazioni che portano a ponderare la finalità del controllo, la trasparenza del trattamento e la centralità che deve essere sempre garantita alla dimensione umana nella sorveglianza.
In particolare, l'indagine deve prendere avvio dalle tutele vigenti volte a limitare sotto l'aspetto "procedurale" l'acquisizione dei dati (facendo riferimento all'art. 4 dello Statuto dei Lavoratori) e il loro utilizzo (previste dalla normativa *privacy*).

1.2. La disciplina del controllo a distanza

Il rapporto di lavoro non è un rapporto contrattuale pari agli altri, essendo in esso insita e imprescindibile la supremazia di una parte sull'altra.
Ciò traspare in modo evidente nel modello originalmente delineato dal Codice civile che riconosceva al datore di lavoro ampi poteri di direzione, controllo e disciplinari solo latamente limitati dalla contrattazione collettiva e da alcuni diritti riconosciuti al lavoratore.

La disuguaglianza viene presa in considerazione dalla Carta costituzionale che, in riferimento al lavoro, non finge un'equità inesistente[133] offrendo specifiche garanzie a tutela del lavoratore, ovvero alla parte contrattualmente più debole. La Costituzione, nel ponderare i differenti interessi in gioco subordina[134] la libertà di iniziativa economica (di cui all'art. 41 Cost.) alle libertà fondamentali del lavoratore (art. 41 comma 2 Cost.).
I principi costituzionali di tutela vengono attuati anche mediante la Legge 300 del 1970 (Statuto dei Lavoratori) in cui gli equilibri e i poteri presenti nel rapporto di lavoro mutano rispetto al modello proposto dal Codice civile.
Lo Statuto salvaguarda il lavoratore vincolando l'esercizio dei poteri datoriali che non possono più essere esercitati in maniera assoluta e arbitraria.
Tra questi, anche il potere di controllo a distanza dell'attività lavorativa viene limitato nel suo esercizio e vincolato a precisi limiti interni ed esterni affinché possa considerarsi legittimo.
Lo Statuto con la previsione dell'art.4 circoscrive i limiti, soggettivi e oggettivi, entro i quali il datore di lavoro può esercitare il potere di controllo a distanza, distinguendo forme e tipologie del relativo esercizio.
La prima formulazione dell'art. 4 SL (rubricata "Impianti audiovisivi") prevedeva:
"*1. È vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori.*
2. Gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti.
3. Per gli impianti e le apparecchiature esistenti, che rispondano alle caratteristiche di cui al secondo comma del presente articolo, in mancanza di accordo con le rappresentanze sindacali aziendali o con la commissione interna, l'Ispettorato del lavoro provvede entro un anno dall'entrata in vigore della presente legge, dettando all'occorrenza le prescrizioni per l'adeguamento e le modalità di uso degli impianti suddetti.
4. Contro i provvedimenti dell'Ispettorato del lavoro, di cui al precedente secondo e terzo comma, il datore di lavoro, le rappresentanze sindacali aziendali o, in mancanza di queste, la commissione interna, oppure i sindacati dei lavoratori di cui al successivo art. 19 possono ricorrere, entro 30 giorni dalla comunicazione del provvedimento, al Ministro per il lavoro e la previdenza sociale".

L'articolo disponeva, innanzi tutto, il divieto assoluto del controllo diretto**[135]**, ovvero del controllo fine a sé stesso, da intendersi quale attività di supervisione rivolta a verificare l'esecuzione della prestazione lavorativa e l'esatto adempimento della stessa.
Il divieto di controllo diretto includeva anche i comportamenti tenuti dal lavoratore durate l'orario di lavoro che esorbitavano il momento tecnico funzionale della subordinazione, ossia quegli atteggiamenti che possono essere definiti come "licenze comportamentali"[136].

---

133 In merito Crisafulli V., *Diritti di libertà e poteri dell'imprenditore*, in *Rivista Giuridica del Lavoro (RGL)*, n. 1, 1954, pp. 69 ss.; Zagrebelsky G., *Giustizia costituzionale*, Il Mulino, Bologna, 2012.
134 In merito Zagrebelsky G., *Giustizia costituzionale*, Il Mulino, Bologna, 2012.
135 Cfr. Alvino I.*, I nuovi limiti al controllo a distanza dei lavoratori nell'intersezione fra regole dello Statuto dei lavoratori e quelle del codice della privacy*, in *Labour & Law Issues (LLI)*, vol. 2, n. 1, 2016, p. 5.
136 In merito Ichino P., *Diritto alla riservatezza e diritto al segreto nel rapporto di lavor*o, Giuffrè Editore, 1979, Milano, pp. 67 e 71 ove definisce la "zona riservata" al lavoratore.

La disposizione normativa introduceva, infatti, un divieto di controllo "a distanza" dell'attività dei lavoratori[137] che è concetto distinto e di ampiezza maggiore rispetto all'attività lavorativa strettamente intesa richiamata nell'art. 3 SL (dedicato ai controlli in presenza).
Il divieto inerisce, quindi, anche tutti gli atteggiamenti e i comportamenti tenuti dal lavoratore nel tempo di lavoro, ma all'esterno del perimetro oggettivo della prestazione.
L'accezione, secondo l'interpretazione giurisprudenziale[138], comprende anche le licenze comportamentali, le pause o i luoghi distinti da quelli di lavoro sebbene adiacenti o connessi (come spogliatoi, servizi o parcheggi).
La norma tutelava, così, la dignità[139] e la riservatezza del lavoratore, vietando che fosse assoggettato ad un controllo volto esclusivamente a sorvegliarlo, attuando un monitoraggio costante all'insaputa dello stesso[140].
L'oggetto immediato del divieto è, pertanto, la persona fisica del lavoratore per tutto il tempo in cui è in attività presso il luogo di lavoro.

Il controllo a distanza acquisiva, però, la dimensione di liceità quando diretto a soddisfare esigenze datoriali, tassativamente elencate dalla norma, e individuate nelle finalità[141] organizzative e produttive e di sicurezza del lavoro, nonché ove l'installazione fosse stata oggetto di autorizzazione da parte del sindacato o dell'Ispettorato del lavoro.
In forza di quanto precisato dal primo comma dell'art. 4 SL, l'interesse del datore all'esatto adempimento della prestazione lavorativa risultava espunto dalle esigenze organizzative dell'impresa, configurandosi come prerogativa distinta.
Veniva, dunque, ammesso il controllo preterintenzionale[142], ovvero quello giustificato in forza di un bilanciamento astrattamente compiuto dal Legislatore tra le esigenze di buon funzionamento dell'impresa e di tutela della privatezza del lavoratore.
La norma vietava, dunque, il controllo a distanza fine a sé stesso fissando un necessario vincolo di funzionalità del monitoraggio.

---

137 Il concetto di "attività dei lavoratori" comprende non solo i comportamenti attuativi della prestazione lavorativa, ma include ogni comportamento posto in essere dal lavoratore nel corso dell'orario di lavoro. Cfr. Corte di Cass. del 18 aprile 2012 n. 16622; Alvino I, *L'art. 4 Stat. lav. alla prova di internet e della posta elettronica*, in *Diritto delle Relazioni Industriali. (DRI)*, n. 4, 2014 p. 1007.

138 Per una definizione di "attività dei lavoratori" tra le molte si rinvia a Corte di Cass., sez. pen, 8 ottobre 1985, n. 8687; Corte di Cass., sez. civ., 3 luglio 2001, n. 8998, Corte App. Torino, 28 marzo 2006; Trib. Genova 1° ottobre 1983.

139 La dignità viene definita come la qualità ontologica che lega il soggetto alla famiglia umana e che definisce i suoi appartenenti in un rapporto paritario. La dignità di un uomo si traduce, quindi, nella libertà come autonomia nella determinazione dei propri. fini. Da ciò si può dedurre che "*la mortificazione della dignità consegue a situazioni in cui si palesa la soggezione di un uomo ad un altro con privazione della libertà di autodeterminazione ed è perpetua quando l'uomo viene ridotto a strumento. (…) Nella relazione di lavoro subordinato, per carattere strutturale della soggezione, risulta connaturato il "germe della sopraffazione" e il rischio di pregiudizi di dignità*". Così Casillo R., *La dignità nel rapporto di lavoro*, in *Rivista di Diritto Civile*, n. 5, 2008, p. 597.

140 Cfr. Grandi M., Pera G., *Sub Art. 4*, in *Commentario alla Statuto dei lavoratori*, Cedam, Padova, 1972, p.9.

141 Romagnoli U., *Sub Art. 4*, in Ghezzi G., Mancini G. F., Montuschi L., Romangnoli U. (a cura di) *Statuto dei diritti dei lavoratori*, Ed. Universitaria, Bologna, 1972, pp. 16-22.

142 Con la definizione di "controlli preterintenzionali" ci si riferisce a quei "controlli indiretti" che ineriscono "qualunque forma di monitoraggio posta in essere dal datore di lavoro per mezzo di impianti che sono espressamente rivolti al soddisfacimento di almeno una delle ragioni di legge, ma dal quale derivi la possibilità di un'indiretta verifica a distanza dell'attività dei lavoratori". In tal senso Dessì O., *Il controllo a distanza sui lavoratori. In nuovo art. 4 Stat. lav.*, Edizioni Scientifiche Italiane, Napoli, 2017, p. 69.

Quando la sorveglianza veniva esercitata in ragione di esigenze oggettive (ed effettive) normativamente previste, il datore di lavoro poteva legittimamente disporre delle informazioni acquisite, anche per eventuali provvedimenti disciplinari[143].
La norma impediva, quindi, il monitoraggio diretto (lesivo della dignità e della riservatezza del lavoratore), ammettendo solo quello giustificato da esigenze normative e preventivamente autorizzato dalle organizzazioni sindacali o dall'Autorità amministrativa.
Nulla, però, diceva in merito alla sorte delle informazioni acquisite mediante un monitoraggio preterintenzionale e utilizzabili anche per fini disciplinari.

1.3. La *ratio* della norma

La *ratio* che ha portato alla stesura dell'originario art. 4 SL inerisce "*la dimensione personalistica, l'intenzione di tutelare la privatezza del lavoratore di fronte all'occhio scrutatore e onnipresente di un Grande Fratello aziendale*"[144].
Come si legge nella Relazione governativa al d.d.l. sullo Statuto dei Lavoratori "*il divieto di utilizzazione di mezzi di controllo a distanza tra i quali, in primo luogo, gli impianti televisivi parte dal presupposto che la vigilanza sul lavoro, ancorché necessaria nell'organizzazione produttiva, vada mantenuta in una dimensione "umana", e cioè non esasperata dall'uso di tecnologie che possono rendere la vigilanza stessa continua e anelastica, eliminando ogni zona di riservatezza e di autonomia nello svolgimento del lavoro*".
Il controllo ammesso è, dunque, quello esercitato dall'uomo sull'uomo e non dalla macchina sull'uomo.
Diversamente "*un siffatto controllo su ogni momento dell'attività lavorativa, magari anche sulle pause del lavoro, non può in alcun modo svolgersi senza una palese compressione dell'attività dei prestatori di lavoro e senza una clamorosa violazione della dignità umana. Una cosa è il controllo del sorvegliante, che interviene, contesta direttamente un'infrazione, dà modo al lavoratore di difendersi, di prospettare le sue ragioni; altra cosa è il controllo anonimo, odioso, spinto fino all'esasperazione, da parte di un meccanismo controllato soltanto dalla direzione*"[145].

Ratio che resterebbe "inossidabile"[146] anche a seguito dell'intervenuta riscrittura dell'art. 4 SL dato che la tutela della dignità e della riservatezza del lavoratore costituisce un limite oggettivo invalicabile[147] nell'esercizio dei poteri datoriali.

Il controllo a distanza trova pertanto i propri limiti quando fuoriesce da quella dimensione umana che deve mantenere nonostante l'interposizione della tecnologia.
La dottrina ha articolato tale concetto, descrivendo l'illiceità del controllo a distanza quando esercitato in modo:

- pervasivo/omnipervasivo. È tale il controllo continuativo e incessante che si rivela lesivo del "diritto alla tranquillità" del lavoratore[148] il quale "*deve poter lavorare serenamente, senza sentirsi costantemente sotto sorveglianza e monitorato in ogni atteggiamento della sua persona*"[149]. Pervasività

[143] A memoria dell'art. 2104 c.c., infatti, l'inadempimento del lavoratore può manifestarsi in maniere differenti quali la mancata o non corretta esecuzione della prestazione, la non ottemperanza dell'orario di lavoro o l'assenza ingiustificata, l'utilizzo del luogo o degli strumenti di lavoro in modo difforme alle istruzioni ricevute, l'appropriazione di beni aziendali.
[144] D'Antona M., *L'art. 4 dello Statuto dei Lavoratori ed elaborati elettronici*, in De Luca-Tamajo R., Imperiali-D'Afflitto R., Pisani. C., Romei R. (a cura di), *Nuove tecnologie e tutela della riservatezza del lavoratore*, Giuffrè Editore, Milano, 1988, pp. 204-205.
[145] Smuraglia C., *Progresso tecnico e tutela della personalità del lavoratore*, in Rivista Giuridica del Lavoro, Vol. 1, 1960, p. 312.
[146] Cfr. Frattini R., Maurelli R., *La nuova disciplina dei controlli a distanza nel dialogo fra art. 4 e Codice privacy*, in *Lavoro e previdenza oggi*, 11-12/2020, p. 715.
[147] Cfr. Santucci R., *La quarta rivoluzione industriale e il controllo a distanza dei lavoratori*, in *Il Lavoro nella giurisprudenza*, n. 1, 2021, p. 25.
[148] Gragnoli E., *L'informazione nel rapporto di lavoro*, Giappichelli Editore, Torino, 1996, p. 167.
[149] Levi A., *Il potere di controllo dell'imprenditore sull'uso degli strumenti di lavoro e le tecnologie informatiche,* in *Un diritto in evoluzione. Studi in onere di Yasui Suva,* a cura di L. Montuschi, Giuffrè Editore, Milano 2007, p. 410.

ricondotta anche alla possibilità riconosciuta al "potere informatico" del datore di lavoro di eseguire un trattamento automatizzato (in particolare, di elaborazione elettronica e di interconnessione) dei dati dei lavoratori[150].

- Continuativo, ovvero perdurante nel tempo, da intendersi come durata costante e attuabile in qualunque momento[151]. Parte della dottrina riconduce al concetto di vessatorietà e pervasività del controllo e a quello di continuità. Il controllo a distanza sarebbe, pertanto, vietato ove l'aspetto della "strumentalità" sia connesso a quello della continuità. "*In altre parole, un controllo che sia soltanto strumentale, ma non continuativo, deve considerarsi assolutamente legittimo*"[152].
- Anelastico[153], facendo riferimento alla rigidità e minuziosità del monitoraggio[154] capace di registrare anche i momenti di distrazione e di disimpegno che sono naturalmente presenti nel lavoro di chiunque e che si devono tollerare[155] al pari delle licenze comportamentali[156].
- Impersonale[157], in quanto privo della dimensione umana. In tal caso, viene meno il necessario confronto diretto e personale tra il controllore e il controllato, elidendo ogni contatto umano-relazionale[158].
- Vessatorio. Il controllo pone i lavoratori in una condizione oppressiva, registrando anche i momenti di distrazione e di disimpegno che sono naturalmente presenti nel contesto lavorativo e che si devono tollerare[159]. La stessa condizione avviene quando il monitoraggio è eseguito in modo occulto e continuativo[160].
- Subdolo[161], essendo in grado di cogliere anche i momenti di distrazione e disimpegno del lavoratore[162] senza che possa essere dallo stesso percepito.
- Occulto, ossia senza che lavoratore sappia o veda il controllore[163]. Per alcuni autori, il requisito della "non conoscibilità" sarebbe da considerarsi vietato quando compiuto da apparecchi che non comportino un controllo saltuario, attuando una sorveglianza continuativa senza alcun preavviso[164].

---

150 Trojsi A., *Potere informatico del datore di lavoro e controllo sui lavoratori, cinquant'anni dopo*, in *Dirittifondamentali.it*, n. 2, 2020, p. 1414.
151 Russo M., *Quis custodiet ipsos custodes? I "nuovi" limiti all'esercizio del potere di controllo a distanza*, in *Labour & Law Issues (LLI),* vol. 2, n. 2, 2016, p.7; M. L. Vallauri, *È davvero incontenibile la forza espansiva dell'art. 4 dello Statuto ei lavoratori*, in *Rivista Italiana di Diritto del Lavoro*, vol. II, 2008, p.726.
152 Levi A., *Il potere di controllo dell'imprenditore sull'uso degli strumenti di lavoro e le tecnologie informatiche*, in *Un diritto in evoluzione. Studi in onere di Yasui Suwa,* a cura di L. Montuschi, Giuffrè Editore, Milano 2007, p. 411.
153 Termine utilizzato dalla Relazione governativa al d.d.l. sullo Statuto dei Lavoratori ove si legge "*il divieto di utilizzazione di mezzi di controllo a distanza tra i quali, in primo luogo, gli impianti televisivi parte dal presupposto che la vigilanza sul lavoro, ancorché necessaria nell'organizzazione produttiva, vada mantenuta in una dimensione "umana", e cioè non esasperata dall'uso di tecnologie che possono rendere la vigilanza stessa continua e anelastica, eliminando ogni zona di riservatezza e di autonomia nello svolgimento del lavoro*".
154 Russo M., *Quis custodiet ipsos custodes? I "nuovi" limiti all'esercizio del potere di controllo a distanza,* in *Labour & Law Issues (LLI)*, vol. 2, n. 2, 2016, p.7.
155 Pera G., *Sub art. 4*, in Assanti C., Pera G (a cura di) *Commento alla Statuto dei Lavoratori*, Cedam, Padova, 1972, p.26.
156 Bellavista A., *Il controllo sui lavoratori*, Giappichelli Editore, Torino, 1995, p. 65.
157 Termine utilizzato dalla Relazione governativa al d.d.l. sullo Statuto dei Lavoratori.
158 Levi A., *Il controllo informatico sull'attività del lavoratore*, Giappichelli Editore, Torino, 2013, p. 22.
159 Pera G., *Sub art. 4*, in Assanti C., Pera G (a cura di) *Commento alla Statuto dei Lavoratori*, Cedam, Padova, 1972, p.25.
160 Santoro Passarelli G., *Osservazioni in tema di art. 3 e 4 stat. lav*, in *Diritto del Lavoro*, vol. I, 1986p. 491.
161 Cataudella A., *Sub art. 4,* in Prosperetti U. (a cura di), *Commentario della Statuto dei Lavoratori,* Giuffrè Editore, Milano, 1975, p. 78.
162 Cataudella A., *Sub art. 4,* in Prosperetti U. (a cura di), *Commentario dello Statuto dei lavoratori*, Tomo I, Giuffrè Editore, Milano, 1975, p. 78.
163 Levi A., *La ridefinizione dell'assetto regolativo dei controlli a distanza, quale tassello di una più complessiva riforma del diritto del lavoro*, in Levi A. (a cura di), *Il nuovo art. 4 sui controlli a distanza. Lo Statuto dei Lavoratori dopo il Jobs Act*, Giuffrè Editore, Milano, 2016, p. 2.
164 Fregni A., Giugni G., *Lo Statuto dei Lavoratori. commentario alla legge 20 maggio 1970 n. 300,* Giuffrè Editore, Milano, 1971, p. 10.

Limiti imposti al controllo a distanza già dal momento in cui i dati vengono acquisiti e memorizzati[165].

1.4. La riscrittura dell'art. 4 SL

L'avvento di nuove tecnologie e il fenomeno della datificazione del lavoro ha comportato l'esigenza di procedere ad una "*revisione della disciplina dei controlli a distanza sugli impianti e sugli strumenti di lavoro, tenendo conto dell'evoluzione tecnologica e contemperando le esigenze produttive ed organizzative dell'impresa con tutela della dignità e della riservatezza del lavoratore*" (art. 1, co. 7, lett. f, Legge n. 183/2014).

Il progressivo sovrapporsi fino a giungere ad una strutturale coincidenza dello strumento di lavoro e di quello di controllo hanno reso, quindi, necessario (e urgente) un intervento normativo che tenesse conto di tale circostanza.

L'evoluzione tecnologica ha introdotto, infatti, strumenti digitali dotati di connettività di rete, caratterizzati da una natura plurifunzionale[166], ovvero abilitati a un'intrinseca capacità di monitoraggio.

Tale condizione ha scardinato i paradigmi su cui si fondava la tutela dell'originario art. 4 SL, portando ad una riformulazione della norma con il c.d. Jobs Act[167].

L'art. 23 del d.lgs. 14 settembre 2015, n. 151, innovando la disciplina, ha dunque disposto che:

"*1. L'articolo 4 della legge 20 maggio 1970, n. 300 è sostituito dal seguente: «Art. 4 (Impianti audiovisivi e altri strumenti di controllo). - 1. Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo gli impianti e gli strumenti di cui al periodo precedente possono essere installati previa autorizzazione della Direzione territoriale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più Direzioni territoriali del lavoro, del Ministero del lavoro e delle politiche sociali.*

2. La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.

---

165 Tullini P. (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Giappichelli Editore, Torino 2017, p. 8.

166 In tal senso Tullini P. (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, G. Giappichelli Editore, Torino 2017, p. 105; Marazza M., *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore)* in *WP CSDLE "Massimo D'Antona".it* – 300/2016, p. 107, www.lex.unict.it; Marazza M., *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore), in Argomenti di Diritti del Lavoro (ADL), vol. 21, n. 3,* 2016, pp. 483 ss.; Dessì O., *Il controllo a distanza sui lavoratori. Il nuovo art. 4 Stat. Lav.*, Edizioni scientifiche Italiane, Napoli 2017, pp. 91 e ss.

167 Tra i molti contributi dedicati alla riscrittura dell'art. 4 SL si rinvia a Del Punta R., *La nuova disciplina dei controlli a distanza sul lavoro,* in *Rivista Italiana di Diritto del Lavoro*, n.1, 2016, pp. 77 ss.; Maio V., *La nuova disciplina dei controlli a distanza sull'attività dei lavoratori e la modernità post panottica,* in Argomenti di Diritti del Lavoro, n.6, 2015, pp. 1186 ss.; Alvino I.*, I nuovi limiti al controllo a distanza dei lavoratori nell'intersezione fra regole dello Statuto dei lavoratori e quelle del codice della privacy*, in *Labour & Law Issues (LLI)*, vol. 2, n. 1, 2016, pp. 1 ss.; Maresca A., *Jobs Act, come conciliare potere di controllo e tutela della dignità e riservatezza del lavoratore,* in *Forum Tuttolavoro (web),* 2016; Sitzia A., *Il controllo (del datore di lavoro) sull'attività dei lavoratori: il nuovo art. 4 st. lav. e il consenso del lavoratore*, in *Labour & Law Issues (LLI)*, vol. 2, n. 1, 2016, pp. 11 ss.; Caricci M. T., *Il controllo a distanza dell'attività dei lavoratori dopo il "Jobs Act" (art. 23 D.Lgs. 151/2015): spunti per un dibattito,* in *Labour & Law Issues (LLI)*, vol. 2, n. 1, 2016, editoriale; Ficari L., *I controlli effettuati attraverso gli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa,* in Levi A. (a cura di), *Il nuovo art. 4 sui controlli a distanza. Lo statuto dei lavoratori dopo il Jobs Act,* Giuffrè Editore, 2016, pp. 99 ss.; Bellavista A., *Il nuovo art. 4 dello Statuto dei lavoratori,* in Zilio Grandi G., Biasi M. (a cura di), *Commentario breve alla riforma "Jobs Act",* WK Cedam, 2016, pp. 717 ss.; Levi A., *La ridefinizione dell'assetto regolativo dei controlli a distanza, quale tassello di una più complessiva riforma del diritto del lavoro*, in Levi A. (a cura di), *Il nuovo art. 4 sui controlli a distanza. Lo statuto dei lavoratori dopo il* Jobs Act, Giuffrè Editore, 2016, pp. 2 ss.; Marazza M., *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore), in Argomenti di Diritti del Lavoro, vol. 21, n. 3,* 2016, pp. 483 ss.; Maresca A., *Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 dello Statuto dei lavoratori*, in Rivista *Italiana di Diritto del Lavoro,* vol. 1, 2016, pp. 513 ss.; Sitzia A., *Personal computer e controlli "tecnologici" del datore di lavoro nella giurisprudenza,* in *Argomenti di Diritto del Lavoro (ADL)*, 2017, pp. 804 ss.; *Zoli C., Il controllo a distanza dell'attività dei lavoratori e la nuova struttura dell'art. 4, legge n. 300/1970, in Variazione sui Temi di Diritto del Lavoro, n. 4, 2016, pp. 635 ss.;* Tullini P. (a cura di), *Controlli a distanza e tutela dei dati personali dei lavoratori*, Giappichelli Editore, Torino, 2017.

3. Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196.»".
L'art. 5, comma 2, del d.lgs. 24 settembre 2016, n. 185, ha ulteriormente previsto che: "*All'articolo 4, comma 1, della legge 20 maggio 1970, n. 300 il terzo periodo è sostituito dai seguenti: «In mancanza di accordo, gli impianti e gli strumenti di cui al primo periodo possono essere installati previa autorizzazione delle (recte: "della") sede territoriale dell'Ispettorato nazionale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali, della sede centrale dell'Ispettorato nazionale del lavoro. I provvedimenti di cui al terzo periodo sono definitivi».*

La riscrittura dell'art. 4 L. n. 300 del 1970 ha (ri)confermato la regola per cui il controllo a distanza dell'attività lavorativa è illegittimo ove esercitato in modo diretto[168], ovvero rivolto a finalità esclusivamente di controllo, risultando deficitario delle giustificazioni indicate nel primo comma.
Il controllo intenzionale, ovvero quello finalizzato ad accertare l'esecuzione della prestazione lavorativa e gli inadempimenti del prestatore, continua così ad essere vietato[169].
La norma ribadisce, al contempo, la legittimità dei controlli preterintenzionali, ossia quelli svolti per esigenze organizzative-produttive e di tutela della sicurezza del lavoro, implementando la categoria con la finalità di tutela del patrimonio aziendale. Come nella precedente versione, oltre alla sussistenza di un'esigenza datoriale oggettiva, i controlli possono essere attuati solo a seguito della sottoscrizione dell'accordo sindacale o del conseguimento dell'autorizzazione amministrativa dell'Ispettorato.
La norma innova profondamente la disciplina nel secondo comma, escludendo la necessità di attuare le tutele indicate per gli "strumenti di controllo" nei riguardi dei dispositivi tecnologici utilizzati per rendere la prestazione lavorativa o per registrare gli accessi e le presenze (definibili "strumenti di lavoro").
Ulteriore novità introdotta è la previsione di utilizzabilità delle informazioni raccolte - mediante gli strumenti di controllo o di lavoro - a tutti i fini connessi al rapporto lavorativo, a patto che venga fornita adeguata informativa sulle modalità di utilizzo degli strumenti e di svolgimento dei controlli e venga rispettato di quanto disposto dal D. Lgs. n. 196/2003 (Codice *privacy*).

La nuova formulazione dell'art. 4 SL introduce, così, tre innovazioni rilevanti.
La prima è l'introduzione di una disciplina "binaria" in ragione alla natura degli strumenti utilizzati dai lavoratori, riconducibili ad un concetto di "controllo" o di "lavoro".
La seconda, è la previsione di nuovi limiti al potere di controllo datoriale in riferimento all'utilizzabilità dei dati, individuati nella normativa *privacy* richiamata nel terzo comma.

168 In commento fra i tanti cfr. Frattini R., Maurelli R., *La nuova disciplina dei controlli a distanza nel dialogo fra art. 4 e codice privacy,* in *Lavoro e previdenza oggi*, 11-12/2020, p. 716; Dagnino E., *Tecnologie e controllo a distanza*, in *Diritto delle Relazioni industriali (DRI)*, 2015, pp. 988 ss.; Dessì O., *Il controllo a distanza sui lavoratori. Il nuovo art. 4 Stat. lav.*, Edizioni Scientifiche Italiane, Napoli, 2017; Proia G., *Trattamento dei dati personali, rapporto di lavoro e "l'impatto" della nuova disciplina dei controlli a distanza*, in *Rivista Italiana di Diritti del Lavoro,* vol. 1, 2016, pp. 547 ss; Trojsi A., *Potere informatico del datore di lavoro e controllo sui lavoratori, cinquant'anni dopo*, in *dirittifondamentali.it*, n. 2, 2020, p.1422.
169 In tal senso è la maggioranza della dottrina. Per una ricognizione delle posizioni v. Bandelloni G., *La rimozione del divieto di controllo a distanza: significato e conseguenze*, in *Rivista Giuridica del Lavoro (RGL)*, n. 1, 2018, p. 86; Carinci M. T., *Il controllo a distanza sull'adempimento della prestazione di lavoro*, in Tullini P. (a cura di) *Controlli a distanza e tutela dei dati personali del lavoratore*, Giappichelli Editore, Torino, 2017, pp. 45 ss.

La riscrittura della disciplina sul controllo a distanza si pone, così, in linea con le crescenti potenzialità dei sistemi tecnologici che consentono, talvolta in maniera intrinseca, un controllo dell'attività lavorativa[170].
La norma introduce, infine, una nuova esigenza a giustificazione del controllo indiretto, ovvero la "tutela del patrimonio aziendale", che si affianca alle finalità organizzative-predittive e di salute e sicurezza del lavoro già previste dalla legge.

1.4.1. Strumento di lavoro e strumento di controllo

La bipartizione introdotta tra strumenti di controllo e di lavoro prevede che alcuni dispositivi possano essere utilizzati senza necessità di accordo autorizzatorio (sindacale o amministrativo), in virtù dell'intrinseca inscindibilità delle due funzioni.
La deroga, secondo la dottrina maggioritaria[171] interesserebbe, infatti, solo la necessità di ottenere l'autorizzazione, dovendo sempre sussistere una delle esigenze indicate al comma 1 dell'art. 4 SL.
E d'altro canto, quale strumento di lavoro sarebbe se non ci fosse almeno la finalità produttiva/organizzativa a giustificarne l'utilizzo?
Il controllo intenzionale continua, così, ad essere vietato come confermato anche dalla Giurisprudenza della Corte di Cassazione nella sentenza del 4 novembre 2021, n. 31778.
La Suprema Corte, nella pronuncia richiamata, ha vagliato la legittimità dell'istallazione di un sistema di videocamere apposte per scopi precipuamente organizzativi e, in particolare, di "pubblicità" delle sedute di esame per conseguire la patente di guida.
Secondo la Giurisprudenza le telecamere, anche se abilitate solo potenzialmente a controllare a distanza la prestazione lavorativa, realizzano *de facto* un controllo diretto.
Di conseguenza, l'impianto di sorveglianza - proprio perché abilitato a esercitare un controllo - soggiaceva a tutti requisiti previsti dall'art. 4 SL, inclusa la necessaria preventiva concertazione.
La Corte afferma, dunque, che "(…) *la nuova formulazione* (ndr. comma 1 art. 4 SL)*, facendo riferimento all'autorizzabilità di apparecchiature dalle quali «derivi anche la possibilità di controllo a distanza», rende chiaro che il fine di controllo a distanza dell'attività non è mai sufficiente a legittimare, da solo (controllo diretto), il controllo sull'attività lavorativa, analogamente a quanto prevedeva la formulazione originaria dell'art. 4, mentre lo è, ferma l'autorizzazione, quale possibilità conseguente ad altri fini (controllo indiretto)*".

L'attenzione del Legislatore della riforma si è, così, concentrata sull'analisi del concetto di strumento destinato a rendere la prestazione.
La nozione di strumento di lavoro risulta, però, complessa da definire, non esistendo una definizione ontologica dello stesso.
La natura "lavorativa" è stata, quindi, ricondotta da parte della dottrina alla destinazione che il datore di lavoro attribuisce al dispositivo dotato di capacità polifunzionali (ovvero contestualmente abilitato a funzioni di lavoro e controllo) quando questo viene affidato al dipendente per svolgere la propria mansione[172].

---

170 In merito Sartori A., *Il controllo tecnologico sui lavoratori. La nuova disicplianitaliana tra vincoli sovranazionali e modelli comportamentali,* Giappichelli Editore, Torino, 2020 pp. 243 ss.; Trojsi A., *Potere informatico del datore di lavoro e controllo sui lavoratori, 50 anni dopo,* in *dirittifondamentali, it*, n. 2, 2020.
171 In dottrina si parla di "valutazione *ex ante* di legittimità dell'installazione" delle apparecchiature operata dal legislatore. In merito Zoli C., Villa E., *Gli strumenti di registrazione degli accessi e delle presenze*, in *Controlli a distanza e tutela dei dati personali del lavoratore*, P. Tullini (a cura di), Giappichelli, Torino, 2017, p. 135 in cui si legge che "*Il legislatore ha, al riguardo, ritenuto che l'impiego dei dispositivi di cui al co. 2 sia sorretto dalle ragioni oggettive elencate nel co. l, alla luce di una valutazione effettuata ex ante*".
172 Marazza M., *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore),* in *Argomenti di Diritto del Lavoro (ADL),* vol. 21, n. 3, 2016, p. 491; Maresca A., *Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 dello statuto dei lavoratori,*

Ciò ha portato la dottrina a dividersi tra chi proponeva una lettura estensiva della nozione di "strumento di lavoro", includendo non solo gli strumenti strettamente necessari per rendere la prestazione lavorativa[173], tesi accolta dalla dottrina maggioritaria, ma anche quelli che costituiscono un mero ausilio[174], tesi rimasta minoritaria.

Quando uno strumento di lavoro possiede intrinseche funzionalità di controllo è, inoltre, necessario - per altri interpreti - valutare se l'apparecchio sia destinato esclusivamente a realizzare l'esecuzione della prestazione lavorativa, oppure soddisfi esigenze più ampie (per esempio di carattere organizzativo) che travalichino il mero adempimento individuale. Il discrimine sarebbe, così, da intendere non solo nella indispensabilità dello strumento per rendere la prestazione, bensì anche nella dimensione "superindividuale" del medesimo quale parte dell'ingranaggio aziendale[175].
Quest'ultima interpretazione appare calzante per comprendere l'effettiva natura dei nuovi strumenti digitali impiegati per gestire il personale o per il compimento della prestazione virtuale, come possono essere le *Digital Workplace*.
Quest'ultime, infatti, costituendo ambienti di lavoro virtuali, risultano certamente essenziali per rendere la prestazione lavorativa a distanza. Di conseguenza, dovrebbero essere definite come strumenti di lavoro. Si deve, però, considerare che le *Digital Workplace* sono in grado di effettuare analisi e di rendere *report* che risultano funzionalmente utili all'organizzazione e non al singolo lavoratore per svolgere la prestazione.
Considerando, dunque, la dimensione "superindividuale" del dispositivo, la natura della *Digital Workplace* varia da "strumento di lavoro" a "strumento di controllo", almeno in riferimento a quegli applicativi che appaiono funzionali all'organizzazione.

Una tesi dottrinale ancora più restrittiva (seppur minoritaria), imporrebbe l'applicazione della disciplina di cui all'art. 4 comma 1 ogni volta che lo strumento abbia insite potenzialità, seppur minime, di controllo. Conseguentemente, la natura di strumento di lavoro sarebbe riservata solo a quei dispositivi scevri di qualsiasi capacità di monitorare l'attività del lavoratore[176].
Rifacendosi all'esempio prima proposto, secondo tale ricostruzione, le *Digital Worplace* dovrebbero essere considerate esclusivamente "strumenti di controllo".

---

in *Rivista Italiana del Diritto del Lavoro (RIDL),* vol. 1, 2016, p. 532; Dessì O., *Il controllo a distanza sui lavoratori,* Edizioni Scientifiche Italiane, Napoli, 2017, p. 91 – 93; Ingrao A., *Il controllo a distanza sui lavoratori*, Cacucci Editore, Bari, 2018, pp. 192 -193.

173 La dottrina maggioritaria identifica, quindi, come strumenti di lavoro solo quelli strettamente necessaria rendere la prestazione lavorativa. In questo senso Del Punta R., *La nuova disciplina dei controlli a distanza sul lavoro (art. 23, d. lgs. n. 151/2015*), in *Rivista Italiana del Diritto del Lavoro (RIDL),* vol. 1, 2016, pp. 101-102; Dessì O., *Il controllo a distanza sui lavoratori*, Edizioni Scientifiche Italiane, Napoli, 2017, p. 94-95; Tullini P., *Il controllo a distanza attraverso gli strumenti per rendere la prestazione lavorativa. Tecnologie di controllo e tecnologie di lavoro: una distinzione possibile?* in Tullini P. (a cura di, in), *Controlli a distanza e tutela dei dati personali del lavoratore*, Giappicheli Editore, Torino, 2017, p. 106; Dagnino E. *Tecnologie e controlli a distanza*, in *Diritto delle Relazioni Industriali (DRI),* n. 4, 2015, p. 991; Stizia A., *Personal computer e controlli "tecnologici", del datore di lavoro nella giurisprudenza*, in *Argomenti di Diritto del Lavoro (ADL)*, 2017, pp. 824-825; Stizia A., *I controlli a distanza dopo il "Jobs Act" e la Raccomandazione R(2015)5 del Consiglio d'Europa*, in il *Lavoro nella Giurisprudenza*, n. 7, 2015, p. 671; Carinci M. T., *Il controllo a distanza sull'adempimento della prestazione di lavoro,* in Tullini P. (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Giappicheli Editore, Torino, 2017, pp. 45 ss.

174 A tale tesi si contrappone altra parte della dottrina (rimasta minoritaria) per cui potrebbero essere considerati "strumenti di lavoro" anche quelli che costituiscono un mero ausilio alla prestazione lavorativa. In tal senso Marazza M., *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore),* in *Argomenti di Diritto del Lavoro (ADL),* vol. 21, n. 3, 2016, p. 483; Maresca A., *Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 dello statuto dei lavoratori,* in *Rivista Italiana del Diritto del Lavoro (RIDL)*, vol. 1, 2016, p. 512; Maio V., *La nuova disciplina dei controlli a distanza sull'attività dei lavoratori e la modernità post panottica,* in *Argomenti di Diritto del Lavoro (ADL)*, n. 6, 2015, p. 1186.

175 Sartori A., *Il controllo tecnologico sui lavoratori*, Giappichelli, Torino, 2020, pp. 248-249.

176 Arbore A., *La nuova disciplina dei controlli ex art. 4 St. lav.*, in Ghera E., Garofalo D. (a cura di), *Semplificazioni sanzioni, ispezioni nel Jobs Act 2,* Cacucci Editore, Bari, 2016, p. 162.

A fornire un chiarimento in merito a cosa debba essere considerato "strumento di lavoro" è intervenuto il Ministero del Lavoro e delle Politiche Sociali che, con Comunicato 18 giugno 2015, ha specificato che "*l'espressione «per rendere la prestazione lavorativa» comporta che l'accordo o l'autorizzazione non servono se, e nella misura in cui, lo strumento viene considerato quale mezzo che «serve» al lavoratore per adempiere la prestazione; ciò significa che, nel momento in cui tale strumento viene modificato (ad esempio, con l'aggiunta di appositi software di localizzazione o filtraggio) per controllare il lavoratore, si fuoriesce dall'ambito della disposizione: in tal caso, infatti, da strumento che «serve» al lavoratore per rendere la prestazione il pc, il tablet o il cellulare divengono strumenti che servono al datore per controllarne la prestazione. Con la conseguenza che queste «modifiche» possono avvenire solo alle condizioni ricordate sopra: la ricorrenza di particolari esigenze, l'accordo sindacale o l'autorizzazione"*.
Dalla definizione di strumento di lavoro sarebbero, così, esclusi i sistemi che *"rappresentino un elemento «aggiunto» agli strumenti di lavoro, non utilizzati in via primaria ed essenziale per l'esecuzione dell'attività lavorativa*"[177].

Concordemente a tale interpretazione, il Garante per la Protezione dei Dati Personali ha ricondotto alla nozione di strumenti di lavoro solo i "*servizi, software o applicativi strettamente funzionali alla prestazione lavorativa, anche sotto il profilo della sicurezza*"[178], mentre si devono intendere "di controllo" le strumentazioni *hardware* e *software* configurate in modo da poter identificare l'utente mediante collegamento univoco tra i dati relativi alla connessione di rete e il lavoratore che la utilizza (come URL, IP *o Mac Address*[179]) e capaci di trattare dati di dettaglio svolgendo, così, un tracciamento[180].
Per il Garante, quindi, un sistema abilitato a tracciare, filtrare o monitorare l'attività informatica comporta una sorveglianza dell'attività del dipendente e qualifica il dispositivo come strumento di controllo[181].

L'analisi per individuare la natura dello strumento deve, quindi, essere effettuata in concreto, caso per caso o, ancor meglio (in ragione dello sviluppo tecnologico), applicativo per applicativo[182].
Ciò al fine di verificare se il dispositivo, da cui derivi la possibilità di controllo, sia, anche senza la funzione di sorveglianza "*ugualmente utilizzabile dal lavoratore per adempiere esattamente l'obbligazione lavorativa: se la risposta è negativa, si rientra nel campo di applicazione del 2° comma (strumento di lavoro), mentre, se la risposta è positiva si potrà rientrare nell'ambito del 1° comma (strumento di controllo), a condizione che il controllo sia giustificato da esigenze organizzative e produttive, o di sicurezza del lavoro o di tutela del patrimonio aziendale*"[183].

Quindi un *software* qualificato in origine come "gestionale" (quale può essere un sistema CRM) deve essere valutato nelle singole funzionalità al fine di comprenderne le potenzialità (e la natura) di controllo.

---

177 Ispettorato Nazionale del Lavoro, Circolare n. 2 del 7 novembre 2016 avente ad oggetto "*Indicazioni operative sull'utilizzazione di impianti GPS ai sensi dell'art. 4, commi 1 e 2, L. n. 300/1970*".
178 GPDP Provvedimento n. 303 del 13 luglio 2016, doc. web. n. 5408460, confermato dal Tribunale di Chieti, sentenza n. 672 del 24 ottobre 2019.
179 GPDP provvedimento del 13 luglio 2016, n. 303, doc. web. n. 5408460 in cui il *Mac Address* viene inteso come indirizzo associato a ciascuna scheda di rete che è integrata in qualsiasi *personal computer* o dispositivo mobile; si tratta di un identificativo univoco che viene impostato dal proprietario *hardware* della singola scheda.
180 GPDP Provvedimento n. 65 del 5 febbraio 2015, doc. web. 3812428.
181 Nel caso oggetto del Provvedimento n. 65 del 5 febbraio 2015, il trattamento dei dati personali dei dipendenti avveniva per mezzo di sistemi *software* che consentivano in modo autonomo e senza che l'utente lo percepisse (c.d. *back-ground*) di monitorare, tracciare, filtrare e controllare in modo indiscriminato e continuo gli accessi a *Internet* o al servizio di posta elettronica dei dipendenti.
182 Anche la giurisprudenza si è espressa sulla necessità di "scomporre" lo strumento informatico in tutti i suoi componenti e applicativi rispetto ai quali dovrà essere indagata la singola potenzialità di controllo. In merito Trib. Torino, sez. lav., n. 1664/2018; Tri. di Padova, sez. lav. del 22 gennaio 2018; Trib. di Savona del 1° marzo 2018; Trib. di pescara del 25 ottobre 2017; Trib. di Milano del 24 ottobre 2017.
183 Grillo Pasquarelli F., *Gli strumenti di controllo a distanza dei lavoratori*, Relazione tenuta all'incontro di studio "Jobs Act *dopo 5 anni: un quadro aggiornato della giurisprudenza*", organizzato dalla SSM, Scandicci, 13 - 15 gennaio 2020.

Valutazione che è stata compiuta anche dal Garante per la Protezione dei Dati Personali che, nel provvedimento dell'8 marzo 2018, ha chiarito che il *software* gestionale Saleforce Arcadia - impiegato da Sky Italia Network Service S.r.l. - non poteva essere considerato "*strumento utilizzato dal lavoratore per rendere la prestazione lavorativ*a" data la sua intrinseca polifunzionalità (che lo abilitava al controllo) [184].
Il sistema, infatti, non si limitava a fornire un supporto ai dipendenti mediante un'anagrafica, ma consentiva ulteriori elaborazioni che permettevano di ricostruire, indirettamente, l'attività effettuata dagli operatori.

1.4.2. Tutela del patrimonio aziendale e controlli difensivi

Un'ulteriore considerazione merita l'introduzione della nuova esigenza di controllo connessa alle finalità di tutela del patrimonio aziendale.
Il nuovo art. 4 SL ha così posto un bilanciamento tra l'interesse del datore di lavoro a tutelare il patrimonio, materiale e immateriale[185], dell'impresa e quello di riservatezza del lavoratore.
La nuova previsione ha portato una conseguente ridefinizione della nozione di "controlli difensivi", ovvero di quei controlli attuati per la tutelare i beni aziendali che esulano dall'ambito di operatività dell'art. 4 SL[186].

La nozione di "controlli difensivi" non è definita dalla legge, ma costituisce un "*tertium genus*"[187], introdotto dalla giurisprudenza[188], che si distingue rispetto al controllo diretto (vietato ai sensi dell'art. 4 co. 1 SL) e preterintenzionale (ammesso per le finalità elencate dall'art. 4 comma 1 SL).
Il concetto di "controllo difensivo" nasce per l'esigenza di accertare una condotta illecita del lavoratore[189] quale elemento fattuale distinto e autonomo rispetto all'esecuzione della prestazione lavorativa.
Il concetto di controllo difensivo fu introdotto per la prima volta dalla Corte di Cassazione, sez. lav. 4746/2002 la quale definì che "*ai fini dell'operatività del divieto di utilizzo di apparecchiature di controllo a distanza*

---

184 Questo perché "*il sistema non si limita a consentire la mera associazione tra la chiamata e l'anagrafica del cliente per facilitare l'attività di gestione richiesta (come si trattasse di un mero archivio informatico ad uso dei soli rapporti con la clientela), ma consente "ulteriori elaborazioni" (es. memorizzazione di dati personali, anche degli operatori, ed estrazioni di report) relativi all'attività telefonica in generale ad opera di diverse funzioni aziendali. Ciò consente di ricostruire, anche indirettamente, l'attività effettuata dagli operatori e rappresenta un sistema idoneo a realizzare controllo, anche solo potenziale e in via indiretta, dell'attività lavorativa*". GPDP provvedimento dell'8 marzo 2018, doc. web n. 8163433.
185 L'espressione "patrimonio aziendale" deve essere intesa secondo un'accezione ampia, non limitata solo al complesso dei beni aziendali, ma comprensiva dell'" immagine esterna" dell'impresa, accreditata presso il pubblico. In tal senso Corte di Cass. 23 febbraio 2012, n. 272. In dottrina Alvino I., *I nuovi limiti al controllo a distanza dell'attività dei lavoratori nell'intersezione fra le regole dello Statuto dei lavoratori e quelle del Codice della privacy*, in *Labour & Law Issues (LLI)*, vol. I, n. 2, 2016, p. 18 per cui la nozione vada intesa in senso ampio, ricomprendendovi "*non solo i beni materiali, ma anche i beni immateriali (immagine, know-how, brevetti, ecc.), tra i quali può essere annoverato il complesso dei rapporti che sono essenziali per lo svolgimento dell'attività produttiva*". Conformemente Del Punta R., *La nuova disciplina dei controlli a distanza sul lavoro (art. 23, D. Lgs. n. 151/2015)*, in *Rivista Italiana di Diritto del Lavoro*, vol. I, 2016 pp. 85 ss.
186 I controlli difensivi sono, infatti, volti ad accertare illeciti dei dipendenti estranei al rapporto di lavoro. In merito tra le molte Corte di Cass. 23 febbraio 2010 n. 4375.
187 Anche se parte della dottrina ha argomentato che i controlli difensivi "*non costituiscono una species estranea allo Statuto, ma sono riconducibili all'area del controllo preterintenzionale*". Così Tullini P., *Comunicazione elettronica, potere di controllo e tutela del lavoratore,* in *Rivista Italiana del Diritto del Lavoro*, vol. 1, 2009, p. 329; conformemente Zoli C., *Il controllo a distanza del datore di lavoro: l'art. 4, l. n. 300/1970 tra attualità ed esigenze di riforma*, in *Rivista Italiana di Diritto del Lavoro*, vol. 1, 2009, p. 500.
188 La categoria dei "controlli difensivi" è stata elaborata dalla giurisprudenza inizialmente in riferimento all'art. 3 SL facendo riferimento ai controlli effettuati dal datore di lavoro diretti ad accertare condotte illecite dei lavoratori. Cfr. Corte di Cass. 7 febbraio 1983, n. 9167; Corte di Cass. 14 luglio 2001, n. 9567; Corte di Cass. 7 giugno 2003, n. 9167; Corte di Cass. 4 marzo 2014, n. 4984.
La categoria è stata successivamente estesa, nella vigenza del vecchio art. 4 SL, alle condotte illecite dei lavoratori offensive del patrimonio aziendale. Cfr. Corte di Cass. 3 luglio 2001, n. 8998; Corte di Cass. 3 aprile 2002, n. 4746.
189 Per una recente analisi sui controlli difensivi si rinvia a Ingrao A., *Il controllo difensivo sugli atti illeciti dei lavoratori da parte di agenzie investigative tra Statuto dei lavoratori, Testo Unico di Pubblica Sicurezza e normativa a protezione dei dati personali,* in *Labor,* n. 1, 2023, pp. 69 ss.

dell'attività dei lavoratori" ci cui all'art. 4 SL "*è necessario che il controllo riguardi (direttamente o indirettamente) l'attività lavorativa, mentre devono ritenersi certamente fuori dall'ambito di applicazione della norma (…) i controlli diretti ad accertare condotte illecite del lavoratore (c.d. controlli difensivi)*".
La Corte di Cass. sez. lav. 15892/2007 ha, successivamente, limitato l'ambito di operatività dei controlli difensivi alle sole condotte "extra lavorative"[190], riconoscendo la necessaria operatività delle tutele statutarie per gli illeciti che siano attinenti o correlati allo svolgimento delle mansioni.

Il richiamo ai "controlli difensivi" è stato più volte adottato dalla Suprema Corte anteriforma per giustificare il controllo svolto da un datore di lavoro, in modalità occulte, a tutela del proprio patrimonio aziendale.
A riguardo la Suprema Corte ha precisato che "*le garanzie procedurali imposte dall'art. 4, secondo comma, della legge n. 300 del 1970 (…) trovano applicazione anche ai controlli c.d. difensivi, ovverosia a quei controlli diretti ad accertare comportamenti illeciti dei lavoratori, quando tali comportamenti riguardino l'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro e non la tutela dei beni estranei al rapporto stesso, dovendo escludersi che l'insopprimibile esigenza di evitare condotte illecite da parte dei dipendenti possa assumere portata tale da giustificare un sostanziale annullamento di ogni forma di garanzia della dignità e riservatezza del lavoratore*"[191] .
Il discrimine tra l'applicabilità o meno delle tutele statutarie risiede, quindi, nell'estraneità dei beni e della condotta illecita rispetto al rapporto di lavoro.
Conformemente a tale principio, la Corte di Cassazione[192] ha, per esempio, ritenuto legittimi i licenziamenti disciplinari comminati da un'azienda ad alcuni dipendenti, addetti alla sorveglianza, a seguito dell'acquisizione di filmati registrati con telecamere installate presso un'altra ditta.
Nel caso analizzato, i controlli posti in essere dal datore di lavoro sono stati giudicati "difensivi" e, in quanto tali, estranei alla disciplina dell'art. 4 SL. Potevano, quindi, essere eseguiti anche in assenza della preventiva autorizzazione sindacale o ammnistrativa.
I controlli - ancorché occulti - erano, inoltre, stati compiti nel rispetto della dignità e della riservatezza dei lavoratori[193].

A seguito della novella del 2015, con dell'introduzione della tutela del patrimonio aziendale quale finalità abilitante al controllo a distanza, la dottrina si è interrogata se i "controlli difensivi" fossero stati assorbiti nel primo comma dell'art. 4 SL e risultassero, così, sempre assoggettati alla preventiva autorizzazione[194].

---

190 Ricostruzione accolta anche dalla giurisprudenza di legittimità successiva. Cfr. Corte di Cass. 23 febbraio 2012, n. 2722; Corte di Cass. 1° ottobre 2012, n. 16622; Corte di Cass. 5 ottobre 2016, n. 20440; Corte di Cass. 10 novembre 2017, n. 26682).
191 Corte di Cass. 23 febbraio 2010, n. 4375.
192 Corte di Cass. 28 gennaio 2011, n. 2117. Nel caso, le immagini rilevavano che i dipendenti licenziati erano entrati abusivamente nell'ufficio dell'impresa attigua, titolare delle videocamere che avevano eseguito le riprese.
193 La Suprema Corte ha in più occasioni precisato che, anche i controlli difensivi, devono svolgersi nel rispetto dei principi di dignità e riservatezza, ovvero in maniera discontinua, non pervasiva e senza eccedere lo scopo per cui erano stati svolti. Tra le tante cfr. Corte di Cass. 28 gennaio 2011, n. 2117.
194 In merito Ingrao A., *Il controllo disciplinare e la privacy del lavoratore dopo il Jobs Act*, in *Rivista Italiana di Diritto del Lavoro*, fasc. 1, p. 46, nota a Corte di Cass. sez. lav. 19922/2016 che nega la possibilità, dopo la riforma del 2015, dei controlli difensivi occulti. Concordemente Ingrao A*, I controlli difensivi tra passato e presente: privacy del lavoratore e inutilizzabilità dei dati*, in *La nuova giurisprudenza civile commentata*, n. 4, 2019, pp. 652 ss; Frattini R., Maurelli R., *La nuova disciplina dei controlli a distanza nel dialogo fra art. 4 e Codice privacy*, in *Lavoro e previdenza oggi*, 11-12/2020, p. 717; Del Punta R., *La nuova disciplina dei controlli a distanza sul lavoro (art. 23 d. lgs. n. 151/2015)*, in *Rivista Italiana di Diritto del Lavoro*, vol. 1, 2016, p. 85; Baletti E., *I poteri del datore di lavoro tra legge e contratto*, relazione tenuta in occasione delle Giornate di Studio Aidlass, Napoli, 16-17 giugno 2016, in www.aidlass.it, p. 40; Trojsi A., *Potere informatico del datore di lavoro e controllo sui lavoratori, cinquant'anni dopo*, in dirittifondamentali.it, n. 2, 2020, p. 1429.

Secondo altri, invece, nulla sarebbe cambiato in riferimento alla categoria dei controlli difensivi che rimarrebbero esenti da ogni tipo di filtro preventivo[195].
Secondo una terza interpretazione proposta, l'attenzione dell'interprete deve incentrarsi non tanto sul fine del controllo (difensivo o meno) ma sul mezzo tecnologico per effettuare il controllo. Conseguentemente, se il dispositivo "*rientra negli impianti di cui al comma 1, il datore deve eseguire il preventivo iter sindacale/amministrativo; se si tratta di strumenti adoperati per lo svolgimento della prestazione (…) vale la disciplina dei commi 2. In entrambi i casi resta fermo il rispetto di quanto stabilito dal terzo comma dell'art. 4 Stat. lav."*[196].

La questione è stata affrontata dalla Suprema Corte nella sentenza del 22 settembre 2021, n. 25732 in cui, giudicando la legittimità di un licenziamento disciplinare[197], ha richiamato la categoria dei "controlli difensivi" nonostante la vigenza della nuova esigenza di "tutela del patrimonio aziendale".
Nella sentenza la Corte ha affermato che, con il nuovo art. 4 SL, i controlli aventi ad oggetto il patrimonio aziendale sono sempre assoggettati ai presupposti di legittimità indicati nel comma prima e ai limiti il cui esercizio è vincolato.
La Corte aggiunge, però che "*occorre tuttavia distinguere tra i controlli a difesa del patrimonio aziendale che riguardano tutti i dipendenti (o gruppi di dipendenti) nello svolgimento della loro prestazione di lavoro che li pone a contatto con tale patrimonio, controlli che dovranno necessariamente essere realizzati nel rispetto delle previsioni dell'art. 4 novellato in tutti i suoi aspetti e "controlli difensivi" in senso stretto, diretti ad accertare specificamente condotte illecite ascrivibili - in base a concreti indizi - a singoli dipendenti, anche se questo si verifica durante la prestazione di lavoro. Si può ritenere che questi ultimi controlli, anche se effettuati con strumenti tecnologici, non avendo ad oggetto la normale attività del lavoratore, si situino, anche oggi, all'esterno del perimetro applicativo dell'art. 4"*.
La Suprema Corte riconosce così la permanenza, anche nel quadro normativo odierno, della fattispecie dei controlli difensivi, ora definiti controlli difensivi "in senso stretto" e distinti da quelli "in senso lato" riconducibili all'art. 4 SL.
Nel caso dei controlli difensivi "in senso stretto" il necessario bilanciamento dei differenti interessi vantati (datore di lavoro-lavorare) deve essere ponderato in concreto secondo un giudizio attuato "*ex post*" e non preventivamente come avviene per quelli afferenti all'art. 4 SL.
Pertanto *"per essere in ipotesi legittimo, il controllo "difensivo in senso stretto" dovrebbe quindi essere mirato, nonché attuato ex post, ossia a seguito del comportamento illecito di uno o più lavoratori del cui avvenuto compimento il datore abbia avuto il fondato sospetto, sicché non avrebbe ad oggetto l'attività - in senso tecnico - del lavoratore medesimo*."
La Corte individua, così, il criterio di necessaria anteriorità temporale del sospetto concreto di adempimento di un illecito rispetto all'inizio dell'attività di controllo.
La raccolta delle informazioni da parte del datore di lavoro deve, quindi, avvenire successivamente all'ipotetico illecito che determina l'esigenza di "controllo difensivo in senso stretto".
Resta, invece, irrilevante il momento di lettura e di analisi dei dati[198].

---

195 Cfr. Maresca A., *Jobs Act, come conciliare potere di controllo e tutela della dignità e riservatezza del lavoratore,* in *Forum Tutto lavoro Ipsoa*, 2016, p. 1; Maio V., *La nuova disciplina dei controlli a distanza sull'attività dei lavoratori e la modernità post panottica*, in *Argomenti di Diritto del Lavoro (ADL)*, vol. 6, 2015, p. 1220.

196 Russo M., *Quis custodiet ipsos custodes? I "nuovi" limiti all'esercizio del potere di controllo a distanza,* in *Labour & Law Issues (LLI),* vol. 2, n. 2, p. R23. Per l'autrice, i controlli difensivi possono essere esercitati rimanendo in una "dimensione umana" e non tecnologica, per esempio, attraverso l'impiego di investigatori privati. In giurisprudenza cfr. Corte di Cass. 31 ottobre 2013, n. 24580; Corte di Cass., 14 febbraio 2011, n. 3590.

197 Nel caso di specie, il licenziamento disciplinare era stato comminato per fatti emersi a seguito di accesso al *computer* aziendale di una lavoratrice da cui venivano acquisiti e trattati dati relativi la cronologia del *browser Google Chrome*. Cfr. Corte di Cassazione 22 settembre 2021, n. 25732.

198 Conformemente, il Tribunale di Treviso con sentenza n. 186 del 2019 ha ritenuto che "*la raccolta dati attraverso la posta elettronica finalizzata ad accertare l'esistenza di illeciti quali quelli ipotizzati nella lettera di contestazione debba considerarsi legittima e non lesiva della normativa sulla privacy con utilizzabilità dei dati raccolti anche nell'ambito del rapporto di lavoro*".

Secondo l'elaborazione giurisprudenziale, la nuova formulazione dell'art. 4 SL ammette un controllo datoriale sull'attività del dipendente per la tutela del patrimonio, nella misura in cui siano esperite le procedure previste dai commi 1 e 3 della norma. Tale ipotesi integra la fattispecie del "controllo difensivo in senso lato".
Diversamente, quando il datore di lavoro abbia maturato il sospetto circa il compimento da parte del lavoratore di possibili condotte pregiudizievoli, attuate a danno del patrimonio aziendale, questi potrà procedere a compiere "controlli difensivi in senso stretto" anche senza integrare le prescrizioni di cui l'art. 4 SL.
In questo caso, però, il datore di lavoro dovrà essere in grado di provare l'anteriorità del sospetto della commissione di un illecito, nonché la sua fondatezza. I dati utilizzabili saranno, infatti, solo quelli acquisiti posteriormente a tale momento.
La Suprema Corte[199] in merito rileva che "*il controllo ex post non può riferirsi all'esame e all'analisi di informazioni acquisite in violazione delle prescrizioni di cui all'art. 4 ST prima dell'insorgere del "fondato sospetto", poiché, in tal modo opinando, l'area del controllo difensivo di estenderebbe a dismisura, con conseguente annientamento della valenza delle predette prescrizioni*".
Diversamente, il datore di lavoro potrebbe "*acquisire per lungo tempo ininterrottamente ogni tipologia di dato, provvedendo alla relativa conservazione e poi invocare la natura mirata (ex post) del controllo incentrato sull'esame e analisi di quei dati*".

La liceità dei controlli difensivi è soggetta, pertanto, alla sussistenza di alcune condizioni.
Innanzitutto, i controlli devono trovare fondamento in un "sospetto qualificato" di una condotta illecita o in concreti indizi di illiceità.
L'oggetto del controllo deve, inoltre, incentrarsi su una condotta del lavoratore estranea a quella lavorativa o inerente all'esecuzione della mansione[200].
I controlli devono, poi, essere determinati da una necessità indifferibile allo stato dei fatti[201] e avviati *ex post*, ovvero "*dopo l'attuazione del comportamento in addebito, così da prescindere dalla mera sorveglianza sull'esecuzione della prestazione lavorativa*"[202].
Il monitoraggio, inoltre, deve essere indirizzato a verificare un comportamento specifico e non una condotta generica[203] . Non dovrà, poi, ledere la riservatezza e la dignità del lavoratore, risultando proporzionato all'obbiettiva esigenza di controllo e condotta per il tempo strettamente necessario.
Infine, il carattere "occulto"[204] dei controlli difensivi deve risultare strumentale all'ottenimento dei risultati a cui sono preordinati, ovvero l'accertamento di una condotta illecita extralavorativa, dato che l'autorizzazione (sindacale o amministrativa) pregiudicherebbe il risultato stesso del controllo. I controlli difensivi devono, pertanto, costituire *l'extrema ratio* da impiegare laddove qualunque altro strumento di controllo non permetta di accertare l'illecito[205].

---

199 Corte di Cassazione del 12 novembre 2021 n. 34092.
200 Cfr. Corte di Cass. sez. lav. 26682/2017; Corte di Cass. sez. pen. 4367/2017; Corte di Cass. sez. trib. 3255/2020.
201 Trib. Roma del 24 marzo 2017 in riferimento ad un controllo difensivo attuato sulla dotazione informatica data in uso al dipendente.
202 Corte Cass. sez. lav. 13266/2018.
203 Crf. Corte Cass. sez. lav. 19922/2016.
204 Cfr. Trib. Torino n. 1664/2018.
205 Gragnoli E., *L'uso della posta elettronica sui luoghi di lavoro e la strategia elaborata dall'Autorità Garante,* in Tullini P. (a cura di) *Tecnologie della comunicazione e riservatezza nel rapporto di lavoro*, in Galgano F. (diretto da), *Trattato di diritto commerciale e diritto pubblico dell'economia*, Cedam, Padova, vol. 1, 2010, p. 62; De Luca Tamajo R., *Introduzione*, in Tullini P. (a cura di) *Tecnologie della comunicazione e riservatezza nel rapporto di lavoro*, in Galgano F. (diretto da), *Trattato di diritto commerciale e diritto pubblico dell'economia*, Cedam, Padova, vol. 1, 2010, p. 6.

1.5. La ridefinizione dei limiti al potere di controllo. Distinzione tra acquisizione e utilizzabilità dei dati: l'adeguata informativa e le tutele *privacy*

La riscrittura dell'art. 4 SL delinea una distinzione tra operazioni che configurano il controllo a distanza (indicate nell'impiego e istallazione degli strumenti) rispetto a quelle relative all'utilizzabilità dei dati acquisiti mediante i dispositivi.

Le informazioni raccolte per effetto dei controlli sono, infatti, utilizzabili in forza di quanto previsto dal comma 3 dell'art. 4 SL *"a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196*".

L'esercizio del controllo (ovvero l'acquisizione delle informazioni) e l'utilizzo dei dati costituiscono, pertanto, due momenti distinti e non un'unica manifestazione del potere datoriale.

La confusione tra i dei due aspetti è stata spesso (erroneamente) sottesa poiché "*frequentemente l'effettuazione del controllo, cioè l'acquisizione del dato, si manifesta in modo visibile soltanto quando si procede alla sua utilizzazione dei confronti del singolo lavoratore*"[206].

La nuova formulazione dell'art. 4 SL definisce chiaramente, invece, la suddivisione di tali fasi, tenendo conto che "*il controllo a distanza si configura esaustivamente nel momento in cui il dato viene acquisito (e memorizzato), anche prescindendo dalla sua utilizzazione che, come detto, è solo eventuale*"[207].

La dottrina qui citata elenca tre fasi cronologicamente distinte in cui si articola la manifestazione del potere e il successivo (solo eventuale) impiego dei dati.

La prima fase inerisce l'acquisizione dei dati, la seconda la loro conservazione e, in fine, la terza – non necessaria – è afferente all'utilizzazione dei dati per la gestione del rapporto di lavoro.

Il potere di controllo si manifesta, quindi, quando lo strumento acquisisce i dati e questi vengono archiviati nel *server*, essendo ininfluente che il datore di lavoro se ne intenda avvalere per la gestione dei lavoratori o che ne conosca la stessa acquisizione.

Delineata la distinzione tra le due funzioni, le condizioni per l'utilizzo dei dati acquisiti, a norma del comma 3 art. 4 SL, sono assoggettate a due adempimenti cumulativi: l'adeguata informativa delle modalità d'uso degli strumenti e di effettuazione dei controlli e il rispetto della disciplina a tutela dei dati personali.

L'adeguata informazione, descrivendo le modalità d'uso degli strumenti e quelle di effettuazione dei controlli, ha la finalità di impedire che venga esercitato un controllo occulto da parte del datore di lavoro.

Attraverso l'informativa, dunque, il lavoratore è posto nella condizione di conoscere le differenti forme in cui può essere sorvegliato, inibendolo dal tenere comportamenti illeciti o sanzionabili disciplinarmente.

L'omessa comunicazione dell'adeguata informativa determina l'inutilizzabilità dei dati acquisiti, come confermato anche dalla sentenza n. 25731 del 22.09.2021[208] della Corte di Cassazione nella cui massima si legge che "*la "chat" aziendale, destinata alle comunicazioni di servizio dei dipendenti, è qualificabile come strumento di lavoro ai sensi dell'art. 4, comma 2, st.lav. novellato, essendo funzionale alla prestazione lavorativa, con la conseguenza che le informazioni tratte dalla "chat" stessa, a seguito dei controlli effettuati dal datore di lavoro, sono inutilizzabili in mancanza di adeguata informazione preventiva ex art. 4, comma 3, st.lav.*"

---

[206] Maresca A., *Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 St. lav.*, in Tullini P. (a cura di) *Controlli a distanza e tutele dei dati personali dei lavoratori,* Giappichelli Editore, Torino, 2017, p. 8.

[207] Maresca A., *Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 St. lav.*, in Tullini P. (a cura di) *Controlli a distanza e tutele dei dati personali dei lavoratori,* Giappichelli Editore, Torino, 2017, p. 8.

[208] Il caso prende avvio da un licenziamento disciplinare comminato a una lavoratrice per avere inviato a una collega, su una "*chat*" aziendale, messaggi offensivi nei confronti di altri colleghi e di un superiore gerarchico. Il datore di lavoro era venuto a conoscenza di tali messaggi in occasione di un controllo tecnico preordinato alla dismissione della *chat*. L'accesso alla *chat* e il relativo controllo non erano, però, stati preceduti da alcuna preventiva comunicazione alla lavoratrice.

La condizione di adeguatezza, non venendo definita dalla norma, è stata oggetto di pronunce giurisprudenziali che hanno fornito un'interpretazione del contenuto dell'informativa affinché questa possa soddisfare il presupposto.
In merito, il Tribunale di Pescara del 25 ottobre 2017, ha precisato che non soddisfa i requisiti della norma "*la dicitura, generica e tautologica, contenuta nel contratto di lavoro di essere a conoscenza delle norme disciplinari relative al rapporto*".
Parimenti, il Tribunale di Torino, con sentenza del 18 settembre 2018 n. 1664, ha indicato che "*l'informativa predisposta ai sensi del comma 3 dell'art. 4 st.lav. dovrà essere dettagliata, specifica e rivolta ai dipendenti non in modo generico, ma in base al loro utilizzo*". Lo stesso giudice di merito ha precisato, analizzando la fattispecie degli accessi *Internet* da parte dei dipendenti, che l'informativa non potrà dirsi adeguata quando *"rivolgendosi alla generalità dei dipendenti, si limiti a prescrivere direttive riguardanti tutte le tipologie di strumenti impiegati nell'organizzazione aziendale. (...). Il lavoratore, invero, deve essere informato del fatto che una sua specifica attività (si pensi agli accessi a Internet) può essere controllata dal datore di lavoro secondo modalità che consentono, ad esempio, di verificare la tipologia dei siti Internet visitati ed altresì di accertare la durata degli accessi ai siti medesimi. Tale tipologia di informazione non è stata fornita al signor (...), al quale non è stato detto esplicitamente che i suoi accessi a Internet avrebbero potuto formare oggetto di integrale ricostruzione e analisi da parte del datore di lavoro mediante elaborazione dei file di log della navigazione Web ottenuti da un proxy server o da un altro strumento di registrazione delle informazioni".*
Da ultimo, anche Tribunale di Vicenza del 28 ottobre 2019 ha confermato che "*ai fini del rispetto dell'art. 4, comma 3, Stat. lav. l'informativa ai dipendenti non è adeguata se non esplicita la possibilità di monitoraggio da parte del datore attraverso strumenti tecnologici. La violazione del predetto comma comporta l'inutilizzabilità delle prove così acquisite, dalla quale deriva l'insussistenza del fatto contestato e posto a fondamento del licenziamento*".
Anche la dottrina[209] è concorde nel ritenere che l'informativa per definirsi adeguata non debba limitarsi a un'indicazione sommaria delle modalità d'impiego degli strumenti e di come verranno svolti i controlli, essendo necessaria una esaustiva e puntuale descrizione delle stesse.
L'informativa "adeguata" deve, quindi, risultare chiara, esaustiva, pertinente e comprensibile.
Oltre la condizione di "adeguatezza" anche quella di "conoscibilità" diviene elemento essenziale per l'utilizzo dei dati acquisti.
In merito la giurisprudenza è divisa, indicando da una parte[210] (secondo un'interpretazione restrittiva della norma) l'obbligo di fornire l'adeguata informativa quale presupposto tassativo e indefettibile all'utilizzabilità dei dati; dall'altra[211] (aderendo ad una tesi più permissiva), ammettendo ipotesi di lecito utilizzo dei dati pur in assenza di preventiva informazione.

La seconda condizione che deve essere attuata per poter utilizzare i dati acquisiti è il rispetto di quanto disposto dal D. Lgs. 30 giugno 2003, n. 196, ovvero dal Codice *Privacy*.
Dovrà, quindi, essere resa l'ulteriore informativa ai fini della tutela dei dati personali.

---

209 In tal senso Maresca A. il quale precisa che "*non si tratta, quindi, di redigere un manualetto di istruzioni per l'impiego dello strumento, ma di identificare le modalità del suo utilizzo che comportano l'acquisizione di dati relativi al lavoratore. In poche parole, spiegare come l'uso dello strumento si raccorda con il controllo che ne deriva. (...) appare preferibile un'informazione mirata e non generalizzata, nel senso che tale informazione dovrà riguardare gli strumenti utilizzati (o utilizzabili) dal lavoratore che così vengono ad essere identificati con riferimento ai controlli cui è sottoposto ciascun dipendente (o gruppi di lavoratori che utilizzano gli stessi strumenti)*" in *Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 St. lav.,* in Tullini P. (a cura di) *Controlli a distanza e tutele dei dati personali dei lavoratori*, Giappichelli Editore, Torino, 2017, p. 24.
210 In tal senso Trib. Roma, ord. 13.6.2018.; C. App. Torino, 27.3.2017; Trib. Padova, ord. 19.1.2018; Trib. Roma, 13.6.2018, n. 57668; Trib. Torino 19.9.2018, n. 1664.
211 In tal senso Trib. Roma, ord. 24.3.2017; Trib. La Spezia, 25.11.2016; Trib. Padova, 5.5.2019; Trib. Padova, ord. 22.1.2018; Trib. Padova, ord. 19.1.2018.

La nuova formulazione della norma risulta sempre incentrata a salvaguardare la dignità e la riservatezza del lavoratore a fronte della crescente integrazione di nuove tecnologie nei rapporti di lavoro che potrebbero compromettere tali libertà fondamentali.
Il concetto di riservatezza acquisisce, però, un'accezione "contemporanea" non venendo più inteso come "diritto a essere lasciati soli" ("*right to be alone*").
D'altro canto, il lavoratore nel momento in cui accetta di instaurare un rapporto di lavoro acconsente anche al "*contatto tra le parti che l'esecuzione del programma contrattuale inevitabilmente esige*"[212].
Relazione che in un contesto digitale diviene intrinseca espressione di connessione e connettività.
La tutela garantita dal nuovo comma 3 dell'art. 4 SL è, dunque, a salvaguardia della dimensione sociale della riservatezza che si manifesta con il diritto dell'interessato affinché i propri dati non vengano acquisiti, trattati e utilizzati in maniera pregiudizievole e occulta.
La nuova disciplina tutela, pertanto, i dati personali del lavoratore e i diritti di quest'ultimo nei trattamenti compiuti durante il rapporto di lavoro.

L'intersezione tra le due discipline – diritto del lavoro e tutela dei dati personali – si delinea in un rapporto di *species ad genus*[213], ove generale è la normativa *privacy* e speciale quella statutaria.
Ciò lo si evince dall'art. 88 Regolamento UE 2016/679 che, disciplinando il "Trattamento dei dati nell'ambito dei rapporti di lavoro", dispone che "*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 forza di ciò, in caso di regolazione concorrente, sarà prevalente quella "speciale" prevista dalla normativa nazionale, qual è il comma 3 dell'art. 4 SL.

L'art. 88 del GDPR (unica norma dedicata dal Regolamento al trattamento dei dati personali nel contesto lavorativo[214]) recede così davanti alle norme di rango primario e alle singole esperienze giuslavoristiche e sindacali, affidando alla sussidiarietà e discrezionalità degli ordinamenti nazionali e dei contratti collettivi la facoltà di introdurre norme specifiche sul trattamento dei dati personali nei contesti di lavoro.
La norma elenca, in via semplificativa, i vari ambiti di intervento, che ineriscono l'intero rapporto di lavoro: dall'assunzione alla cessazione. Ciò al fine di adottare "*misure appropriate e specifiche a salvaguardia della dignità umana, degli interessi legittimi e dai diritti fondamentali degli interessati*"[215].
Nella normativa europea si ritrova, così, un lessico noto allo Statuto dei lavoratori, ovvero la salvaguardia della "dignità umana" del lavoratore.
Il principio risulta ora articolato nell'ulteriore espressione di "libertà di autodeterminazione" del dipendente da intendersi quale libertà "positiva" ad avere il dominio attivo sulle proprie informazioni. Tutela che implementa la libertà "negativa" a non essere sorvegliati (già oggetto dell'art. 4 SL).

Coerentemente alle previsioni di cui all'88 GDPR, il Codice *Privacy*, nel rinnovato art. 111, rubricato "Regole deontologiche per trattamenti nell'ambito del rapporto di lavoro", stabilisce che "*il Garante promuove, ai sensi dell'articolo 2-quater, l'adozione di regole deontologiche per i soggetti pubblici e privati interessati al trattamento dei dati personali effettuato nell'ambito del rapporto di lavoro per le finalità di cui all'articolo 88 del Regolamento, prevedendo anche specifiche modalità per le informazioni da rendere all'interessato*".

---

212 P. Ichino, *Introduzione*, in A. Sartori, *Il controllo tecnologico sui lavoratori*, Giappichelli Editore, Torino, 2020, p. XII.
213 In merito Proia G., *Trattamento dei dati personali, rapporti di lavoro e "l'impatto" della nuova disciplina dei controlli a distanza,* in *Rivista Italiana di Diritto del Lavoro*, Fasc. 4, 2016, pp. 547 ss.
214 Cfr. Agenzia dell'Unione Europea per i diritti fondamentali, Consiglio d'Europa, *Manuale sul diritto europeo*, p. 369.
215 Art. 88 par. 2 GDPR.

La norma si collega all'art. 2quater del D. Lgs 196/2003 che invita il Garante per la Protezione dei Dati Personali (GPDP) a promuovere l'adozione di regole deontologiche nelle materie richiamate, previa consultazione pubblica, attribuendo loro anche una determinata efficacia.
Il comma 4 dell'art. 2quater precisa, infatti, che "*il rispetto delle disposizioni contenute nelle regole deontologiche di cui al comma 1 costituisce condizione essenziale per la liceità e la correttezza del trattamento dei dati personali*".
La formulazione sottolinea, così, il passaggio dai "*codici di condotta e di buona condotta*", del vecchio art. 111 Cod. *Privacy*, al nuovo strumento delle "*regole deontologiche*" di natura più agile e caratterizzato da una maggiore libertà di forma[216].
Il fine è proprio quello di agevolare la libertà "positiva" dei lavoratori ad avere il dominio attivo sulle proprie informazioni.

La formulazione dell'art. 2quater del Cod. *Privacy* sembra, però, riconoscere un'efficacia maggiore rispetto a quella prescritta dal GDPR per cui i codici di condotta ove "*si limitano alla corretta applicazione del (…) regolamento, in funzione della specificità dei vari settori*"[217]. Il dettato del Cod. *Privacy* pare, infatti, definirli come una fonte autonoma di diritto oggettivo, discostandosi dal dettato dell'art. 88 GDPR che riserva esclusivamente alla legge e alla contrattazione collettiva il compito di dettare norme *ad hoc* sul trattamento dei dati personali nei rapporti di lavoro[218].
A definire la natura dei Codici di condotta come atti di *soft law* è intervenuto l'European Data Protection Board (EDPB) adottando le Linee guida sui Codici di condotta e le autorità di vigilanza[219].
EDPB definisce i Codici di condotta come "*strumenti di responsabilizzazione volontari che stabiliscono specifiche norme di protezione dei dati per categorie di titolari e di responsabili del trattamento. Essi possono essere un utile ed efficace strumento di responsabilizzazione in quanto forniscono una descrizione dettagliata dei comportamenti più appropriati, in termini giuridici ed etici, con riguardo a un determinato settore. Dal punto di vista della protezione dei dati, i codici possono quindi fungere da decalogo per i titolari e i responsabili del trattamento che progettano e svolgono attività di trattamento dei dati conformi al regolamento, conferendo un significato operativo ai principi di protezione dei dati stabiliti dalla legislazione europea e nazionale*"[220].
Successivamente, il GPDP con provvedimento del 10 giugno 2020, n. 98 ha approvato i requisiti per l'accreditamento degli Organismi di monitoraggio (Odm) dei codici di condotta previsti dal Regolamento europeo, nomina necessaria per l'approvazione di un Codice di condotta da parte del Garante.

Oltre all'introduzione dei Codici di condotta, il Codice *Privacy* racchiude poche altre (sintetiche) indicazioni in riferimento al trattamento dei dati personali nell'ambito dei rapporti di lavoro.
Le prescrizioni, racchiuse negli articoli dal 111 al 115 del Codice, nulla dicono in merito all'informativa che deve essere fornita al lavoratore per l'utilizzabilità dei dati acquisiti, di cui all'art. 4 comma 3 SL.
L'art. 111bis Cod. Privacy riprende il precedente art. 13 comma 5bis del D. Lgs. 196/2003, in merito alla ricezione di *CV,* e prevede che i datori di lavoro possano fornire le informazioni (ex art. 13 GDPR) ai

---

216 In tal senso Busacca A., *Sub art. 88*, in Riccio G. M., Scorza G., Bellisario E. (a cura di), *GDPR e normativa privacy. Commentario,* Wolters Kluwer, Milano, 2018, p. 652.
217 Art. 40 par. 1 GDPR.
218 A riguardo Stizia sottolinea come nella redazione dei Codici di condotta il ruolo delle parti sociali sia soltanto indiretto, mentre il regolamento, indicando i contratti collettivi, vuole senz'altro attribuire una funzione di primo piano agli attori delle relazioni industriali. Stizia A., *Il decreto legislativo di attuazione del Regolamento Privacy (n. 101 del 2018): profili giuslavoristici,* in *Lavoro Diritti Europa*, vol. 1, n. 2, 2018, p.12.
219 EDPB, Linee guida 1/2019 sui codici di condotta e sugli organismi di monitoraggio a norma del regolamento (UE) 2016/679 del 4 giugno 2019. Le Linee guida sono state adottate con lo scopo di fornire assistenza interpretativa in relazione all'attuazione degli articoli 40 e seguenti del GDPR.
220 EDPB, Linee guida 1/2019 sui codici di condotta e sugli organismi di monitoraggio a norma del regolamento (UE) 2016/679 del 4 giugno 2019, p. 7.

candidati al momento del primo contatto utile, successivo all'invio del *CV* stesso. Il consenso al trattamento dei dati contenuti nel *CV* non è dovuto qualora le informazioni siano utilizzate esclusivamente per valutare la convenienza al rapporto di lavoro.
Il previgente art. 112 del D. Lgs. 196/2003 è stato abrogato e assorbito dalle nuove previsioni di cui all'art. 2sexies, comma 2 lett. dd) Cod. *Privacy*[221].
L'art. 113 mantiene fermi i vincoli posti dall'art. 8 SL e conferma la persistenza dei divieti di indagini, sia in ambito privato che pubblico, sulle opinioni dei lavoratori e di compiere discriminazioni a loro discapito (ex art. 10 D.Lgs 10 settembre 2003 n. 276).
L'art. 114 del Codice, volto a regolare i controlli a distanza, esprime un mero rinvio alla normativa statutaria prevedendo che "*resta fermo quanto disposto dall'art. 4 della legge 20 maggio 1070, n. 300*".
Infine, l'art. 115 del Cod. *Privacy* impone al datore di lavoro - nei casi di lavoro domestico, telelavoro e lavoro agile - di garantire ai prestatori il rispetto della loro personalità e libertà morale.

Per trovare indicazioni in merito a come deve essere "l'informativa *privacy*" e alle altre prescrizioni per tutelare i dati personali è necessario far riferimento al Regolamento UE 2016/679 (GDPR).
Il rimando formulato dallo Statuto al Codice *Privacy* italiano determina, al contempo, un implicito richiamo[222] alla disciplina europea a tutela dei dati personali, in ragione delle modifiche apportate al Codice dal Decreto Legislativo 101/2018[223].
Devono, pertanto, intendersi acquisiti dalla disciplina lavoristica i principi ivi fissati e, in primo luogo, il principio di *accountability*, introdotto dall'art. 5, par. 2 GDPR[224]. Quest'ultimo determina la responsabilizzazione del datore di lavoro affinché siano garantite idonee misure tecniche e organizzative a protezione dei dati personali dei lavoratori.
Sono, inoltre, cooptati nella disciplina lavoristica anche gli altri principi indicati dall'art. 5 al par. 1 del GDPR[225] e specificatamente: il principio di liceità, lealtà e trasparenza, di finalità limitata, di

---

221 Art. 2 sexies, comma 2, lett. dd) Cod. Privacy: "*instaurazione, gestione ed estinzione, di rapporti di lavoro di qualunque tipo, anche non retribuito o onorario, e di altre forme di impiego, materia sindacale, occupazione e collocamento obbligatorio, previdenza e assistenza, tutela delle minoranze e pari opportunità nell'ambito dei rapporti di lavoro, adempimento degli obblighi retributivi, fiscali e contabili, igiene e sicurezza del lavoro o di sicurezza o salute della popolazione, accertamento della responsabilità civile, disciplinare e contabile, attività ispettiva*".

222 In dottrina sul tema Carinci M. T., *Il controllo a distanza dell'attività dei lavoratori dopo il "Jobs Act" (art. 23 D. Lgs. 151/2015): spunti per un dibattito,* in Labour & Law Issues, vol. 2, n. 1, 2016, pp. I ss; Ingrao A., *Il controllo disciplinare e la privacy del lavoratore dopo il Jobs Act,* in Rivista Italiana di Diritto del Lavoro, vol. 36, n. 1, 2017, pp. 46 ss.; Alvino I., *I nuovi limiti al controllo a distanza dell'attività dei lavoratori nell'intersezione fra le regole dello Statuto dei lavoratori e quelle del Codice della privacy*, in Labour & Law Issues, vol. 2, n. 1, 2016, pp. 1 ss.

223 Recante "disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)". Per un approfondimento si rinvia a Scagliarini S. (a cura di), *Il "nuovo" codice in materia di protezione dei dati personali,* Giappichelli Editore, Torino, 2019.

224 Art. 5 par. 2 GDPR: Principi applicabili al trattamento di dati personali. 2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»).

225 Art. 5 par. 1 GDPR: "*Principi applicabili al trattamento di dati personali. 1. I dati personali sono:*
a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);
c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);

minimizzazione, di precisione e accuratezza, di limitazione della conservazione e di integrità e riservatezza.
Al GDPR può, inoltre, farsi riferimento ai fini dell'individuazione delle condizioni minime sufficienti per redigere l'informativa, indicate negli artt. 13 e 14 del Regolamento.
L'informativa *privacy* risulterà, quindi, adeguata ove redatta per iscritto, preventivamente al trattamento, in modo conciso, trasparente, intelligibile e facilmente accessibile.
Tra le varie indicazioni che dovrà contenere l'informativa, conformemente agli articoli 5, 13[226] e 14[227] del GDPR, vi è anche la finalità del trattamento a cui i dati sono destinati.

---

f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»)".

[226] Art. 13 GDPR: "I*nformazioni da fornire qualora i dati personali siano raccolti presso l'interessato*
1. In caso di raccolta presso l'interessato di dati che lo riguardano, il titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:
a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
b) i dati di contatto del responsabile della protezione dei dati, ove applicabile;
c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
d) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, paragrafo 1, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali garanzie o il luogo dove sono state rese disponibili.
2. In aggiunta alle informazioni di cui al paragrafo 1, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente:
a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
b) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
c) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
d) il diritto di proporre reclamo a un'autorità di controllo;
e) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.
3. Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente di cui al paragrafo 2.
4. I paragrafi 1, 2 e 3 non si applicano se e nella misura in cui l'interessato dispone già delle informazioni".

[227] Art. 14 GDPR: "I*nformazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato*
1. Qualora i dati non siano stati ottenuti presso l'interessato, il titolare del trattamento fornisce all'interessato le seguenti informazioni:
a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
b) i dati di contatto del responsabile della protezione dei dati, ove applicabile;
c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
d) le categorie di dati personali in questione;
e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un destinatario in un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, paragrafo 1, secondo comma, il riferimento alle garanzie adeguate o opportune e i mezzi per ottenere una copia di tali garanzie o il luogo dove sono state rese disponibili.
2. Oltre alle informazioni di cui al paragrafo 1, il titolare del trattamento fornisce all'interessato le seguenti informazioni necessarie per garantire un trattamento corretto e trasparente nei confronti dell'interessato:
a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
b) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
c) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano e di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
d) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prima della revoca;
e) il diritto di proporre reclamo a un'autorità di controllo;

Tenendo conto che il comma 3 art. 4 SL ammette l'utilizzabilità dei dati acquisiti per "*tutti i fini connessi al rapporto di lavoro*", l'informativa dovrà indicare in maniera chiara la possibilità di utilizzare i dati per fini disciplinari.
La mancata previsione della specifica finalità di utilizzo determina, infatti, l'inibizione all'impiego dei dati per uno scopo differente da quello enunciato, salvo che superi il vaglio di cui l'art. 6 par. 4 del GDPR.
La norma da ultimo richiamata prevede, infatti, che "*al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento tiene conto, tra l'altro: a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto; b) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento; c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'articolo 9, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10; d) delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati; e) dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione*".
L'utilizzo di dati per finalità differenti da quelle indicate nell'informativa implica, pertanto, un'accurata ponderazione delle condizioni di ammissibilità indicate dall'art. 6 comma 4.
Per esempio, se viene indicato nell'informativa che i dati verranno utilizzati per soddisfare esigenze organizzative e produttive, tale finalità sembra difficilmente compatibile con la possibilità di impiegare i dati acquisiti anche per fini disciplinari.
Contrariamente, verrebbe implicitamente ammesso un controllo diretto della prestazione, vietato ai sensi del comma 1 dell'art. 4 SL.
Parimenti, anche ove la finalità di utilizzo indicata sia quelle inerente alla tutela del patrimonio aziendale (che parrebbe ipoteticamente idonea a ricomprendere le correlate finalità di natura disciplinare) i dati non potranno essere impiegati per irrogare sanzioni disciplinari, salvo non si configuri un "controllo difensivo in senso stretto".

---

f) la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico; g) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.
3. Il titolare del trattamento fornisce le informazioni di cui ai paragrafi 1 e 2:
a) entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati;
b) nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato; oppure
c) nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali.
4. Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati ottenuti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni informazione pertinente di cui al paragrafo 2.
5. I paragrafi da 1 a 4 non si applicano se e nella misura in cui:
a) l'interessato dispone già delle informazioni;
b) comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato; in particolare per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatte salve le condizioni e le garanzie di cui all'articolo 89, paragrafo 1, o nella misura in cui l'obbligo di cui al paragrafo 1 del presente articolo rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di tale trattamento. In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni;
c) l'ottenimento o la comunicazione sono espressamente previsti dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento e che prevede misure appropriate per tutelare gli interessi legittimi dell'interessato; oppure
d) qualora i dati personali debbano rimanere riservati conformemente a un obbligo di segreto professionale disciplinato dal diritto dell'Unione o degli Stati membri, compreso un obbligo di segretezza previsto per legge".

1.6. Il principio di proporzionalità nell'esercizio del potere di controllo tecnologico

Il principio di proporzionalità costituisce un canone fondamentale posto a presidio del legittimo esercizio del potere datoriale.

La sua attuazione è ravvisabile in tutte le forme in cui l'esercizio del potere direttivo si può esplicare, come lo svolgimento del controllo o l'erogazione di una sanzione disciplinare.

Il potere datoriale deve, quindi, manifestarsi in modo adeguato allo scopo che si intende soddisfare: sia questo ripristinare l'ordine violato (nel caso della sanzione) o esercitare un controllo sull'attività lavorativa.

Nel caso del potere disciplinare, questo dovrà essere commisurato, nella propria manifestazione, alla gravità della violazione ovvero alla concreta infrazione addebitata al dipendente.

Ciò si evince dallo stesso art. 2106 c.c. che non disegna il potere disciplinare come incondizionato, ma lo affida all'articolazione della contrattazione collettiva, stabilendo che le sanzioni dovranno essere graduate in maniera proporzionata alla gravità delle stesse.

Parimenti, il potere di controllo risulta assoggettato al principio di proporzionalità.

Ciò determina una necessaria ponderazione, da effettuarsi in concreto, sulle forme mediante cui viene esercitato il monitoraggio in relazione alle finalità che il datore di lavoro si prefigge di raggiungere.

Esigenze che sono definite come precondizione per il controllo stesso dallo Statuto e individuate nelle ragioni organizzative-produttive, di sicurezza del lavoro e di tutela a del patrimonio aziendale.

Il principio comporta, quindi, una necessaria valutazione delle forme di controllo attuate e vincola il datore di lavoro a graduare le modalità con cui esercitare la sorveglianza affinché non venga lesa la dignità e la riservatezza dei lavoratori.

L'art. 4 comma 1 SL esige, dunque, una proporzionalità tra l'esercizio del potere di controllo e la tutela della dignità e della riservatezza del lavoratore,[228] ponendo il principio quale "*criterio di moderazione del potere imprenditoriale, potenzialmente lesivo dei diritti fondamentali dell'uomo che lavora*"[229].

Il controllo, anche se fondato su esigenze normativamente riconosciute, dovrà compiersi in modo da ridurre al minimo il sacrificio degli interessi in gioco del lavoratore

Per tale ragione, è necessario valutare in concreto l'effettiva sussistenza delle finalità previste dall'art. 4 comma 1 SL.

Analisi che appare ulteriormente dovuta in ragione delle nuove tecnologie utilizzate dalle imprese nell'ambito della gestione dei rapporti di lavoro.

Come illustrato nel primo capitolo, gli strumenti informatici posti a disposizione dei lavoratori potrebbero essere dotati di intrinseche capacità di monitoraggio, più o meno sofisticate, in relazione alle potenzialità di elaborazione dei dati acquisiti.

È, dunque, necessario valutare preliminarmente se il controllo:

a) sia in grado di raggiungere l'obiettivo proposto, compiendo un giudizio di idoneità sul monitoraggio svolto. Si dovrà, pertanto, valutare se il dispositivo tecnologico sia idoneo a realizzare la specifica finalità per cui il controllo viene attuato.

b) Risulti necessario, nel senso che non sussista altra misura meno invasiva idonea a raggiungere lo scopo con pari efficacia. In questo caso, è necessario stabilire se lo strumento digitale esegua una tipologia di controllo che non possa essere evitata in ragione della singola esigenza di sorveglianza individuata.

---

[228] Cfr. Zoli C., *Il controllo a distanza del lavoratore: l'art. 4 l. n. 300/1970 tra attualità ed esigenze di riforma*, in *Rivista Italiana di Diritto del Lavoro*, n. 4, vol. I, 2009, pp. 485 ss.; Perulli A., *Razionalità e proporzionalità nel diritto del lavoro*, in *Giornale di diritto del lavoro e di relazioni industriali*, vol. 1, 2005, pp. 1 ss.; Russo A., Tufo M., *I controlli preterintenzionali: la nozione*, in Levi A. (a cura di) *Il nuovo art. 4 sui controlli a distanza. Lo statuto dei Lavoratori dopo il Jobs Act*, Giuffrè Editore, Milano, 2016, pp. 53 ss.

[229] Perulli A., *Razionalità e proporzionalità nel diritto del lavoro, in Giornale di diritto del lavoro e di relazioni industriali*, vol. 1, 2005, p. 25.

c) Sia ponderato ed equilibrato, ovvero il monitoraggio apporti più benefici che danni ai differenti interessi in gioco. In questo caso, la valutazione interesserà la proporzionalità in senso stretto del controllo. In tale ipotesi, è opportuno stimare se il controllo compiuto dallo strumento tecnologico risulti strettamente limitato alla finalità di controllo prefissata, venendo svolto in maniera discontinua, non pervasiva e senza eccedere la finalità individuata.

1.7. Il principio di proporzionalità nei controlli difensivi occulti e l'intervento della giurisprudenza della Corte Europea

Il principio di proporzionalità deve essere rispettato anche nel caso dei controlli "difensivi in senso stretto" attuati a tutela del patrimonio aziendale, ovvero "*diretti (…) all'esterno del perimetro applicativo dell'art. 4*"[230].

Il bilanciamento di proporzionalità, in questo caso, si esprimerebbe nel rapporto cronologico tra l'insorgere del "fondato sospetto concreto" e l'avvio del controllo difensivo, in modo che i dati acquisiti e utilizzati siano solo quelli posteriori a tale momento.

Le modalità di svolgimento dei controlli "difensivi in senso stretto" dovranno, inoltre, integrarsi con i principi elaborati dalla Corte Europea dei Diritti dell'Uomo che ha richiamato più volte il necessario bilanciamento tra la *privacy* del singolo e gli interessi di tutela datoriali.

La verifica della "proporzionalità del controllo tecnologico" deve, quindi, tenere in considerazione anche le pronunce della Corte Europea dei Diritti dell'Uomo, poiché i suoi orientamenti influenzano non solo la Corte di Giustizia dell'UE, ma anche i tribunali nazionali[231].

La Corte di Strasburgo, a partire dagli anni 90, ha progressivamente ampliato l'ambito di applicazione dell'art. 8 della Convenzione Europea dei Diritti dell'Uomo (CEDU) inerente al "*diritto al rispetto della vita privata e familiare*".

La Corte nel caso Halford vs. Regno Unito (Corte EDU del 25 giugno 1997, ricorso n. 20605/1992) ha analizzato le modalità di controllo attuate nei confronti di una lavoratrice subordinata mediante intercettazioni telefoniche.

La Corte, nella propria pronuncia, ha ravvisato una violazione dell'art. 8 CEDU, sostenendo che la ricorrente poteva vantare una "*reasonable expectation of privacy*".

La Corte elabora, così, il principio della "ragionevole aspettativa di *privacy*" che un lavoratore può pretendere sul luogo di lavoro e in cui risulta inclusa anche l'attività professionale svolta[232].

La giurisprudenza della Corte EDU sui controlli a distanza mediante strumenti tecnologici subisce una progressiva evoluzione che approda a significativo cambiamento con il caso Bărbulescu vs. Romania[233], (Corte EDU del 5 settembre 2017, ricorso n. 61496/2008).

---

230 Corte di Cass. 12 novembre 2021, n. 34092.

231 Ai sensi dell'art. 117 comma 1 Cost., i diritti sanciti dalla CEDU costituiscono parametro interposto di costituzionalità. Principio sancito dalla pronuncia della Corte costituzionale del 24 ottobre 2007 n. 348 e dalla pronuncia della Corte costituzionale del 24 ottobre 2007 n. 349.

232 Cfr. caso Niemietz vs. Germania, Corte EDU del 16 dicembre 1992, ricorso n. 13710/1988 in cui la Corte EDU conclude che il rispetto della vita privata deve ricomprendere anche il diritto di stabilire relazioni con altre persone, anche nell'ambito professionale, elemento vitale per i rapporti umani. Come si legge nella sentenza non vi è alcuna "*reason of principle why this understanding of the notion of "private life" should be taken to exclude activities of a professional or business nature since it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world*" (par. 29).

233 Sul tema Stizia A., *Personal computer e controlli "tecnologici" del datore di lavoro nella giurisprudenza*, in *Argomenti di Diritto del Lavoro (ADL),* n. 3, 2017, pp. 804 ss.

La fattispecie analizzata dalla Corte interessava il monitoraggio effettuato da un datore di lavoro sull'*account* aziendale *Yahoo Messenger* di un dipendente, creato su indicazione dell'impresa, per finalità esclusivamente professionali. Il controllo aveva condotto al licenziamento del lavoratore in ragione dell'utilizzo improprio fatto dell'*account*, impiegato per fini personali.
Il datore di lavoro aveva, infatti, preventivamente fornito istruzioni in merito all'utilizzo dell'*account* di posta elettronica, che doveva essere destinato esclusivamente per intrattenere rapporti con i clienti, inibendo qualsiasi utilizzo extralavorativo.
Meno chiaro era, invece, il fatto se l'informativa contenesse indicazioni sulle modalità di sorveglianza e sulle finalità (anche disciplinari) di tale controllo.
Nella pronuncia la Corte di Strasburgo riprende le nozioni precedentemente enucleate di "vita privata" e "*reasonable expectation of privacy*", afferenti all'art. 8 CEDU. Valutando il caso concreto ha affermato che, per quanto limitative possono essere le indicazioni fornite dal datore di lavoro, "*an employer's instruction cannot reduce private social life in the workplace to zero*"[234].
La Corte ha proseguito la propria disamina valutando se la Romania avesse costruito un adeguato quadro regolatorio a tutela della *privacy*.
Nel fare ciò, per la prima volta la Corte attribuisce rilievo all'interesse del datore di lavoro al controllo della prestazione, contrapponendolo all'interesse del lavoratore alla riservatezza.
Al fine di controbilanciare tali interessi, la Corte ha formulato un elenco di fattori che le Corti nazionali avrebbero dovuto valutare al fine di evitare abusi di potere a discapito dei lavoratori.
Tra gli elementi da tenere in considerazione vengono menzionate la preventiva informativa al dipendente sulla possibilità di monitoraggio, la natura del controllo, il grado di intrusività del monitoraggio, la durata, l'ambito spaziale e il numero di soggetti interessati.
Devono, poi, essere ponderate le legittime finalità di controllo (che devono essere tanto più pregnanti tanto più intrusivo è il grado di controllo posto in essere) e le conseguenze che il controllo può apportare al lavoratore.

La questione in merito al bilanciamento tra il diritto alla *privacy* del lavoratore e l'interesse al controllo del datore di lavoro, viene nuovamente analizzato nella recente sentenza López Ribalda vs. Spagna ove la Corte ha definito quando sia possibile derogare al principio di necessaria informazione preventiva ai fini dell'utilizzabilità dei dati acquisiti[235].
La Grande Camera della Corte Europea dei Diritti dell'Uomo nella propria sentenza, riformulando la sentenza López Ribalda e altri vs. Spagna del 9 gennaio 2018[236], richiama i criteri espressi nel caso Bărbulescu vs. Romania, adeguandoli alla fattispecie esaminata.

---

234 Bărbulescu vs. Romania., Corte EDU del 5 settembre 2017, ricorso n. 61496/2008, par. 80.
235 Il principio di necessaria informazione e la sua possibile deroga acquisisce particolare rilievo nel caso, per esempio, di controlli tecnologici effettuati da sistemi la cui funzione di sorveglianza costituisca una funzionalità "aggiuntiva" a quelle per cui il *software* è stato inizialmente installato o, addirittura, progettato.
236 Corte EDU, 17 ottobre 2019 (Grand Chamber), ricorsi n. 1874/2013 e n. 8567/2013.
La vicenda analizzata interessava dei furti individuati in un supermercato spagnolo nel 2009.
Il direttore di un supermercato, dopo aver verificato che il livello dei beni in giacenza e i dati sulle vendite non corrispondevano per una differenza di svariate migliaia di euro, decise di installare un sistema di videosorveglianza.
Questo, tuttavia, veniva installato senza previa informazione dei lavoratori e in siti nascosti.
Tramite i filmati acquisiti dalle telecamere, nei dieci giorni successivi, venivano individuati quattordici dipendenti del supermercato che commettevano i furti e, in forza di ciò, licenziati per giusta causa senza preavviso.
cinque dipendenti adivano, però, i tribunali spagnoli contestando il licenziamento intimato sulla base di registrazioni ottenute in violazione del diritto alla riservatezza.
I giudici spagnoli rigettavano il ricorso, valutando legittimo il licenziamento a seguito del *test* di proporzionalità compiuto.
Il controllo esercitato per mezzo del sistema di sorveglianza nascosto doveva, dunque, ritenersi ammissibile dato che lo scopo perseguito con le telecamere era legittimo e la misura adottata era necessaria e proporzionale.

Secondo la Corte Europea dei Diritti dell'Uomo, per garantire la proporzionalità delle misure di controllo adottate nei luoghi di lavoro, nel bilanciamento dei contrapposti interessi, si devono tenere in considerazione i seguenti elementi: 1) l'informativa, chiara e preventiva al monitoraggio che deve essere fornita al lavoratore in merito alle possibilità di controllo; 2) il grado di estensione del monitoraggio e di intrusione nella riservatezza del lavoratore; 3) le ragioni legittime fornite dal datore per giustificare il controllo; 4) la possibilità di installare un sistema di controllo basato su metodi e misure meno intrusivi per la *privacy* del lavoratore, anche alla luce delle circostanze del caso concreto e dello scopo perseguito dal datore; 5) le conseguenze del controllo per il dipendente e l'utilizzo dei dati raccolti da parte del datore, anche rispetto alla compatibilità con la finalità dichiarata; 6) la presenza, specie quando il controllo sia invasivo, di tutele appropriate per il lavoratore (tra le quali l'informativa ai dipendenti o ai rappresentanti sindacali, la dichiarazione a un organismo indipendente dell'adozione di tale misura o la possibilità di fare reclamo).

La Corte di Strasburgo, valutando il bilanciamento tra le contrapposte esigenze, ha ritenuto legittimi i motivi posti alla base del controllo "occulto" datoriale.
La *ratio* del ragionamento, in linea con quanto detto dalla giurisprudenza italiana[237] sui controlli difensivi "in senso stretto", ha considerato ammissibile la sorveglianza diretta all'accertamento di comportamenti illeciti (diversi dal mero inadempimento della prestazione lavorativa) ed effettuata con modalità non invasive della libertà e dignità dei dipendenti.
Principio ribadito anche dalla Giurisprudenza italiana di legittimità, nella sentenza del 22 settembre 2021, n. 25732 della Corte di Cassazione, analizzata in precedenza, che ha ammesso i controlli difensivi ove diretti all'accertamento di comportamenti illeciti diversi dal mero inadempimento della prestazione lavorativa.

1.8. Problemi ancora irrisolti sul controllo tecnologico

La novellata disciplina del controllo a distanza ha sicuramente apportato delle modifiche significative, volte a considerare le nuove potenzialità tecnologiche e i rischi che dall'utilizzo ne possono derivare.
Nonostante ciò, il concetto di controllo a distanza sembra trascurare le reali potenzialità connesse alla datificazione della prestazione e alle capacità possedute dagli strumenti impiegati di misurare, tracciare e analizzare i lavoratori.
Tali abilità ineriscono, in particolar modo, all'utilizzo dei dati per la gestione del rapporto di lavoro e non all'acquisizione degli stessi.
Si deve, infatti, tenere in considerazione che il controllo si manifesta, ai sensi dell'art. 4 comma 1 SL, mediante l'installazione di dispositivi e la raccolta di informazioni e non con l'elaborazione e l'esame dei dati.
Acquisire ed utilizzare dati costituiscono, pertanto, due operazioni distinte ove solo la prima integra i requisiti del potere di controllo.

Tale distinzione, però, potrebbe non soddisfare le esigenze di tutela dei lavoratori a fronte delle potenzialità a cui sono abilitati i nuovi sistemi informatici.
Considerare, infatti, che il potere di controllo si manifesti quando i dati vengono recepiti ha un valore ove questi siano immediatamente comprensibili.
Se viene "osservata" una prestazione "analogica" mediante strumentazione, il controllo ci restituirà immagini, suoni o, comunque, informazioni immeditatamente intellegibili, cioè "autoevidenti".

[237] Da ultimo Corte di Cass. sentenza del 22 settembre 2021, n. 25732.

Quando si passa, però, a controllare una prestazione "nativa digitale", questa non sempre è in grado di restituire informazioni *ictu oculi* comprensibili.
Davanti a informazioni che risultano complesse, non organizzate e il cui significato appare oscuro ove non interpretato, la ponderazione sulla legittimità del controllo potrebbe risultare fallace.
A memoria dell'art. 4 SL, il controllo diretto sul lavoratore è sempre vietato, risultando permesse solo le forme di controllo "preterintenzionale", ovvero quelle scaturenti da esigenze produttive-organizzative, tutela della salute e sicurezza, tutela del patrimonio aziendale.
La valutazione, però, di un controllo "lecito" (in quanto finalizzato a soddisfare una di tali finalità oggettive) potrebbe risultare errata ove i dati non siano interpretati.
Di fatto, potrebbe apparire legittimo un controllo prima dell'elaborazione di dati (in particolare ove "non autoevidenti") e configurarsi come vietato, in quanto "diretto" a sorvegliare la prestazione, a seguito dell'interpretazione.
L'analisi *ex ante* compiuta sulla possibilità di impiegare uno strumento dotato di potenzialità di controllo risulterebbe, così, parziale in riferimento alle reali facoltà del dispositivo informatico.

Le informazioni accumulate dal monitoraggio possono, inoltre, permettere la creazione di enormi *database* sui dipendenti, generando un sistema di banche dati costituito da schede personali a cui accedere per operazioni di *Data Analysis*.
La sorveglianza sul posto di lavoro non è più, quindi, la semplicemente registrazione di informazioni "biografiche" di un dipendente, ma include il tracciamento di dinamiche sociali (ovvero come i dipendenti interagiscono tra loro e con l'organizzazione), le attitudini, eventuali abitudini. Nonché comprendere lo stato psicofisico dei lavoratori, con particolare riguardo allo *stress* lavoro-correlato e al grado di soddisfazione provato.
Informazioni che esorbitano l'ambito strettamente lavorativo di valutazione professionale.
La sorveglianza a distanza si dota, quindi, di nuove potenzialità grazie alla tecnologia dell'informazione e ai sistemi di connessione alla rete che consentono, in tempo reale, l'accesso, l'analisi e lo scambio di informazioni sui processi di lavoro e sui prestatori che li eseguono.

Permangono, così, alcuni problemi irrisolti.
Innanzi tutto, il Legislatore ha definito la nozione di controllo concentrandosi sullo "strumento", tralasciando di analizzare le modalità con cui può essere esercitato il controllo.
Come osservato da parte della dottrina, il Legislatore del 2015 ha incentrato la tutela sulla tipologia degli strumenti utilizzati, piuttosto che sulle modalità del controllo, con il rischio che la normativa si riveli eccessivamente restrittiva nei confronti dei controlli informatici, favorendone un uso improprio[238].
Non vi è dubbio, infatti, che "*i valori in campo siano rimasti inalterati, mentre tutt'altro che omogeneo appare il grado di permeabilità delle norme del Titolo I ai mutamenti organizzativi*"[239].
Le potenzialità di acquisire ed elaborare dati tramite nuovi dispositivi tecnologici evidenziano, quindi, l'opportunità di un aggiornamento normativo che sopporti le differenti esigenze di tutela.
Il lavoro digitale necessita così di nuove indicazioni per un esercizio del potere di controllo che bilanci i contrapposti interessi.
A riguardo occorre interrogarsi se, a eventuali lacune, può soccorrere la lettura coordinata con la normativa *privacy* e, in caso affermativo, fino a che punto.

---

238 In tal senso M. Lanotte, *La ridefinizione dei limiti al potere di controllo a distanza*, in A. Levi (a cura di), *Il nuovo art. 4 sui controlli a distanza. Lo Statuto dei Lavoratori dopo il Jobs Act*, Giuffrè Editore, Milano, 2016, p. 42.
239 Tebano L, *Lavoro, potere direttivo e trasformazioni organizzative*, Editoriale Scientifica, Napoli, 2020, p. 243.

In secondo luogo, la norma trascura l'esistenza e l'utilizzo di dati "non autoevidenti".
La nozione di controllo a distanza, come originariamente intesa, inerisce la possibilità di osservare i lavoratori mediante il supporto di apparecchi.
In un contesto "analogico", ove il prestatore può essere osservato mediante dispositivi audiovisivi o di registrazione della parola, il potere di controllo del datore di lavoro coincide con il momento di acquisizione del dato.
L'utilizzo di strumenti che registrano un'attività lavorativa compiuta "in presenza" restituiscono, infatti, un'informazione immediatamente comprensibile, ovvero "autoevidente", prontamente spendibile dal datore di lavoro.
Il momento in cui viene esercitato il controllo si può intendere come coincidente (da un punto di vista fattuale anche se non normativo) con quello di recepimento del dato, non essendo necessaria alcuna elaborazione intermedia.
Quando, però, si passa ad osservare una prestazione compiuta interamente in un ambiente di lavoro digitale, il binomio "acquisizione del dato - esercizio del potere di controllo" sembra affievolirsi.
La prestazione "nativa digitale", ovvero quella che nasce e si esaurisce in un contesto informatico, non sempre è immediatamente comprensibile.
I dati estrapolati da contesti digitali possono risultare "non strutturati" oppure "di scarico" (come gli *exhaust data)* e, dunque, rivelarsi "non autoevidenti".
Utilizzare dati "non autoevidenti", ovvero elaborarli per renderli comprensibili, potrebbe far sì che il controllo da indiretto si qualifichi, poi, come diretto o sproporzionato.
Acquisire dati "non significativi" sposta il momento "critico" in cui viene esercitato il potere datoriale nella fase successiva di interpretazione. Attività che si realizza mediante il supporto (necessario) di *software* o sistemi di IA.
Il controllo tecnologico verrebbe, così, a compiere un monitoraggio "disumano" (ovvero fatto della macchina sull'uomo[240]) non più a causa del mezzo utilizzato per acquisire le informazioni, ma in ragione del processo di elaborazione. Quest'ultimo, rimesso a sistemi algoritmici o di IA, le cui logiche decisionali possono apparire oscure o arbitrarie.

Infine, non è stata considerata la variazione ontologica dell'esecuzione del lavoro (da analogico a digitale) e la necessità di osservare l'attività lavorativa per fini diversi da quelli disciplinari.
Se la prestazione diviene, infatti, "nativa digitale" sviluppata integralmente in ambienti di lavoro virtuali, l'utilizzo di strumenti informatici diviene l'unico mezzo per poter verificare l'adempimento della prestazione[241].
In merito, è stato osservato che "*il controllo sull'adempimento può rispondere, in via diretta ed esclusiva, a soddisfare un'esigenza organizzativa, di sicurezza sul lavoro (…) o di tutela del patrimonio aziendale. Di conseguenza, ben potrebbe configurarsi l'utilizzo di strumenti che per rispondere ad una o più delle predette finalità comportino "solo" o "anche" il controllo dell'attività lavorativa*"[242].

---

240 Utilizzando il lessico della Relazione governativa al d.d.l. sullo Statuto dei Lavoratori il controllo a distanza deve essere mantenuto in una "*dimensione umana".*

241 In tal senso Bellavista A., *I poteri dell'imprenditore e la privacy del lavoratore*, in Il Diritto del Lavoro, vol. 76, fasc. 3, 2002, pp. 149 ss.; Aimo M., *Privacy, libertà di espressione e rapporto di lavoro*, Jovene, Napoli, 2003, p. 123; Lanotte M., *La ridefinizione dei limiti al potere di controllo a distanza,* in Levi A. (a cura di) *Il nuovo art. 4 sui controlli a distanza. Lo Statuto dei Lavoratori dopo il Jobs Act,* Giuffrè Editore, Milano, 2016, pp.40 – 42.

242 Lanotte M., *La ridefinizione dei limiti al potere di controllo a distanza*, in Levi A. (a cura di) *Il nuovo art. 4 sui controlli a distanza. Lo Statuto dei Lavoratori dopo il Jobs Act*, Giuffrè Editore, Milano, 2016, pp.41 che richiama per le esigenze organizzative Cester C., Mattarolo M. G., *Diligenza e obbedienza del prestatore di lavoro. Art. 2104*, in Schlesinger P. (a cura di), *Il Codice Civile. Commentario*,

Il controllo sarebbe, dunque, svolto al di fuori di un ambito strettamente disciplinare, assumendo le sembianze di un "potere di controllo direttivo"[243].
Questi aspetti appaiono trascurati dalla novella del 2015, apparentemente ancora legata ad una concezione di potere di controllo a distanza preordinata (quasi esclusivamente) all'esercizio del potere disciplinare, "*senza considerare le molteplici finalizzazioni che lo stesso può soddisfare*"[244]. In particolare, ove la prestazione venga svolta attraverso strumenti informatici in ambienti digitali e le informazioni acquisite difettino di comprensibilità immediata.

Le criticità qui richiamate ben spiegano come le nuove tecnologie siano in grado di elaborare nuove informazioni (ritenute "oggettive") da dati inizialmente "neutri" (in quanti privi di significato) grazie a dispositivi che alimentano nuovi flussi informatici generati da una grande eterogeneità di fonti.
Fonti che, nell'ambito della gestione delle risorse umane, hanno ampliato potenzialità, ambito di applicazione e capacità di interpretazione dei dati acquisiti.

Ci si domanda, quindi, se la norma riesca a far fronte a tali problematiche, oppure risultino dei "vuoti di tutela" che devono essere necessariamente presi in considerazione.

Giuffrè Editore, Milano, 2007, pp. 588 ss.. Per la tutela del patrimonio aziendale si rinvia a Levi A., *Il controllo informatico sull'attività del lavoratore,* Giappichelli Editore, Torino, 2013, pp.165 ss.
[243] Cfr. Tebano L., *Lavoro, potere direttivo e trasformazioni organizzative*, Editoriale Scientifica, Napoli, 2020, pp. 239 – 252. In merito si rinvia al capitolo 1 punto 6.
[244] Lanotte M., *La ridefinizione dei limiti al potere di controllo a distanza,* in Levi A. (a cura di) *Il nuovo art. 4 sui controlli a distanza. Lo Statuto dei Lavoratori dopo il Jobs Act*, Giuffrè Editore, Milano, 2016, pp.41.

Capitolo 2
Nuove tecnologie e potere di controllo

Parte 2
Utilizzo di sistemi digitali per la gestione del personale e l'esecuzione della prestazione in ambienti virtuali

2.1. Natura degli strumenti digitali

Come si è avuto modo di argomentare nella ricostruzione svolta, una delle novità più rilevanti introdotte dalla riforma dell'art. 4 SL è stata la ridefinizione dei limiti al potere di controllo datoriale.
Questo, anche se assoggettato ai vincoli della normativa *privacy*, ha derogato alla precedente formulazione[245] consentendo l'utilizzo di strumenti che, pur attuando un controllo a distanza, non manifestano il carattere della vessatorietà.
Il giudizio in merito alla concreta mancanza di tale caratteristica potrebbe, però, risultare inficiato sia per la portata "plurifunzionale" [246] degli strumenti di lavoro, dotati di potenzialità intrinseche di controllo, sia (e soprattutto) per le potenzialità informative insite ai dati grezzi resi intellegibili con l'interpretazione.
In particolare, la raccolta di dati "non autoevidenti" apparentemente "neutri" può convertire un controllo lecito in pervasivo a seguito della loro elaborazione.
La verifica della reale vessatorietà del controllo sarebbe, dunque, riscontrabile solo *ex post,* ovvero quando le capacità informative dei dati siano resi evidenti.

Alla luce di ciò, è necessario in primo luogo sottoporre a un'attenta valutazione i dispositivi tecnologici utilizzati per l'esecuzione della prestazione e per la gestione del personale in ambienti digitali al fine di comprendere se questi possano essere annoverati nella nozione di strumento di lavoro o costituiscano strumenti di controllo.
Si tratta di un approccio qualificatorio[247] che deve prendere in considerazione, inevitabilmente, le funzionalità dei singoli applicativi compiendo accertamenti, anche di natura tecnica, in merito alla natura inscindibile o meno delle potenzialità di controllo.

Compiuta tale preliminare valutazione, si procederà a valutare se il carattere della vessatorietà, apparentemente assente, non si manifesti in maniera tangibile quando i dati grezzi elaborati siano resi intellegibili.

***

Partendo a classificare i dispositivi in riferimento alle loro potenzialità di controllo o di mero supporto all'attività lavorativa si valuteranno le caratteristiche funzionali delle *Digital Workplace*, dei sistemi HRIS, CRM e AST.

---

245 Vallauri M. L., *È davvero incontenibile la forza espansiva dell'art. 4 dello statuto dei lavoratori?,* in *Rivista Italiana di Diritto del Lavoro*, vol. 3, 2008, p. 719.
246 In tal senso Tullini P. (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Giappichelli Editore, Torino 2017, p. 105; Marazza M., *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore),* in *WP CSDLE "Massimo D'Antona".it*– 300/2016, p. 107, www.lex.unict.it; Dessì O., *Il controllo a distanza sui lavoratori. Il nuovo art. 4 Stat. Lav.,* Edizioni scientifiche Italiane, Napoli 2017, pp. 91 e ss.
247 Cfr. Marazza M., *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore)*, in *Argomenti di Diritto del Lavoro (ADL)*, vol. 21, n. 3, 2016, pag. 503.

Cominciando dalle *Digital Workplace*, non può essere negato che il loro utilizzo sia essenziale per lo svolgimento della prestazione lavorativa, soprattutto in quelle realtà ove il lavoro è stato integralmente remotizzato.
La possibilità di svolgere la prestazione in un regime di telelavoro o di lavoro agile diviene possibile anche grazie alla tecnologia delle *Digital Workplace.*
Tramite gli ambienti digitali è, infatti, possibile accedere "virtualmente" al luogo di lavoro ed eseguire la propria attività senza essere fisicamente presente in azienda mantenendo, al contempo, la possibilità di rapportarsi con i colleghi e i superiori tramite le *community* della piattaforma.
Lo stesso dispositivo è, però, integrato con funzionalità aggiuntive che risultano più vantaggiose per l'organizzazione aziendale che a supporto dell'attività del lavoratore.
Le potenzialità rimesse alla piattaforma, per esempio, di analizzare il grado di interazione di un lavoratore con i propri colleghi, il livello di formazione conseguito o il bilanciamento tra tempo di lavoro e di riposo rientrano in funzionalità poste principalmente a sostegno dell'impresa. Si tratta, infatti, di informazioni impiegate per migliorare la gestione dei lavoratori e supportare il *management* nelle decisioni strategiche.
Tali servizi costituiscono un mero ausilio all'esecuzione della prestazione rappresentando un elemento addizionale agli strumenti di lavoro essenziali per l'esecuzione dell'attività lavorativa.
Per tale ragione, le *Digital Workplace,* pur costituendo "strumenti di lavoro" (ai sensi dell'art. 4 comma 2 SL) quando "servono al lavoratore"[248], mutano la propria natura in "strumenti di controllo" ove supportino il datore di lavoro nell'esercizio dei propri poteri di direzione[249].
Dovranno, quindi, considerarsi "strumenti di controllo" tutti gli applicativi della *Digital Workplace* che non si limitino ad assistere in maniera essenziale i lavoratori nella propria attività, rientrando in una dimensione "superindividuale" quale parte dell'ingranaggio aziendale[250].

Proseguendo l'analisi degli strumenti informatici impiegati per la gestione del personale, anche i sistemi di HRIS risultano essere maggiormente funzionali all'amministrazione aziendale che ai singoli lavoratori per l'esecuzione della prestazione.
La creazione di *database* mediante gli HRIS e la successiva analisi dei dati ivi archiviati permette di automatizzare attività specifiche del processo gestionale come la coordinazione degli orari di lavoro, il calcolo dei salari e dei *benefit*, la valutazione delle prestazioni e la mappatura delle competenze.
L'elaborazione dei dati avviene, inoltre, mediante "moduli" aggiuntivi del sistema di HRIS o con *software* esterni di natura statistica, quali possono essere *Excel* e applicativi programmabili (come STATA, SPSS o R).
Le funzioni dei sistemi di HRIS risultano, quindi, ultronee e non essenziali all'esecuzione della prestazione lavorativa e, in taluni casi, non costituiscono nemmeno un mero ausilio.
I risultati delle elaborazioni compiute appaiono, infatti, principalmente funzionali all'organizzazione, grazie alle quali può coordinare la formazione dei lavoratori, pianificare le carriere o attribuire premi di risultato.
I sistemi di HRIS risultano, quindi, integrati al *management* e non all'esecuzione dell'attività lavorativa in senso stretto.

---

248 In dottrina viene rilevato che la ricostruzione della nozione legale dipende dallo specifico contesto organizzativo. "*La formula "utilizzato" implica dunque un accertamento nel merito che evidenzi l'effettivo utilizzo dello strumento da parte del lavoratore al di là dell'astratta utilizzabilità dell'apparecchio per lavorare*". In tal senso Cairo L., *Il controllo a distanza dei lavoratori: precedenti nella giurisprudenza di ieri decisi con la norma di oggi*, in *Labour & Law Issues (LLI)*, vol. 2, n. 1, 2016, p. 72.
249 In tal senso Alvino I., *I nuovi limiti al controllo a distanza dell'attività dei lavoratori nell'intersezione fra regole dello Statuto dei lavoratori e quelle del Codice della privacy*, in *Labour & Law Issues (LLI)*, n. 1, vol. 2, 2016, pp. 24 ss; Stizia A., *Personal computer e controlli "tecnologici" del datore di lavoro nella giurisprudenza,* in *Argomenti di Diritto del Lavoro (ADL),* n. 3, 2017, pp. 804 ss.
250 Sartori A., *Il controllo tecnologico sui lavoratori*, Giappichelli Editore, Torino, 2020, pp. 248-249.

Pertanto, la natura di questi dispositivi risulta estranea al concetto di "strumento di lavoro" allineandosi alle caratteristiche di uno "strumento di controllo".

Anche i sistemi CRM risultano funzionali principalmente (se non prettamente) a finalità imprenditoriali, essendo utilizzati per migliorare il servizio offerto e "fidelizzare" i clienti.
Tale scopo appare diretto a soddisfare interessi unicamente datoriali e non a fornire uno strumento essenziale per eseguire la prestazione lavorativa.
I CRM, inoltre, potendo fornire informazioni indirette sull'operato dei lavoratori (come l'*output* e l'*outcome* conseguiti o i *feedback* ricevuti) pongono, di fatto, il datore di lavoro nella condizione di acquisire informazioni rilevanti sull'attività lavorativa eseguita dai dipendenti, consentendo di elaborare dei "*rating*" sulla base degli elementi quantitativi e qualitativi recepiti.
Anche ai CRM, pertanto, deve essere attribuita la qualifica di "strumento di controllo" nei riguardi dei dati che (indirettamente) possono fornire sui lavoratori.

Da ultimo, i sistemi ATS, impiegati per la ricerca e selezione dei miglior candidati, rispondono esclusivamente a logiche e a interessi imprenditoriali, risultando estranei a qualsiasi impiego per lo svolgimento dell'attività lavorativa.

Tutti i dispositivi tecnologici impiegati per la gestione dei lavoratori o per l'esecuzione digitale della prestazione hanno, pertanto, caratteristiche tali da poterli definire come "strumenti di controllo".

La potenzialità di controllo insita ai dispositivi tecnologici non può, quindi, essere negata e deve essere riconosciuta soprattutto in relazione alle potenzialità di elaborazione a cui sono abilitati[251].

Tenendo conto di quanto esposto, con particolare riguardo alle *Digital Workplace,* ai HRIS e ai CRM, l'atto di "installazione" degli strumenti (indicato dal comma 1 art. 4 SL) coinciderebbe con quello di creazione di un *account* del lavoratore (sulla piattaforma di *Digital Workplace*) o dell'*ID* personale (nel gestionale HRIS o di CRM).
Pertanto, il controllo verrebbe esercitato, avendo riguardo della *ratio* della norma, anche quando le potenzialità di sorveglianza di detti dispositivi non siano volute e/o conosciute dal datore di lavoro.
La natura di strumento di controllo diviene, infatti, preponderante nel momento stesso in cui l'apparecchiatura sia dotata di tale potenzialità, ponendo il datore di lavoro nella possibilità di sorvegliare all'occorrenza il lavoratore.
Le *Digital Workplace* e i sistemi di gestione HRIS e CRM risulterebbero, quindi, "strumenti di controllo" proprio perché dotati di quelle potenzialità di monitoraggio accessibile in maniera discrezionale al datore di lavoro. Gli applicativi di analisi installati in tali sistemi risulterebbero, inoltre, "elementi aggiuntivi" abilitanti al monitorare dell'attività lavorativa ivi svolta[252].

---

[251] Proprio in riferimento a ciò, alcuni autori precisano come i *Software Analytics* "*debbano sempre reputarsi strumenti di controllo, in quanto costituiscono programmi "non nativi" del dispositivo materiale dato in dotazione al lavoratore per eseguire le mansioni. Essi, infatti, non possono servire in alcun modo al lavoratore a rendere la prestazione, ma semmai soddisfano bisogni conoscitivi del datore di lavoro circa la produttività del singolo".* Ingrao A., *Il potere di controllo a distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata*, Cacucci Editore, Bari, 2018, p. 181.

[252] Medesimo orientamento è stato adottato dal Garante per la Protezione dei Dati Personali che ha indicato i *software* mediante i quali è possibile eseguire operazioni di "monitoraggio", "filtraggio", "controllo" e "tracciatura" in maniera costante e indiscriminata degli accessi a Internet e in modalità non percepibili dall'utente (c.d. in *background*) come strumenti di controllo, non potendo essere considerati "*strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa*". A riguardo Garante per la Protezione dei Dati Personali, provvedimento n. 303 del 13 luglio 2016, commentata da Trojsi A., *Al cuore del nuovo art. 4, co. 2, St. Lav.: la delimitazione della fattispecie degli "strumenti utilizzati per rendere la prestazione lavorativa",* in *Rivista Italiana di Diritto del*

Non si può, dunque, negare che i sistemi informatici per la gestione del personale o per l'esecuzione della prestazione digitale siano dotati di potenzialità di tracciatura e analisi tali da connotarne la natura di "sorveglianti".

2.2. La "nuova" fase critica del controllo

Gli strumenti tecnologici a supporto dell'attività lavorativa si stanno evolvendo e l'abilità di elaborazione diviene una fase essenziale per comprendere la "natura" di informazioni talvolta prive di significato.

Davanti a informazioni che risultano "non autoevidenti", complesse e il cui significato appare oscuro ove non interpretato, la ponderazione sulla legittimità del controllo, richiesta dall'art. 4 comma 1 SL, potrebbe risultare fallace negando il carattere di vessatorietà di un controllo invece presente.
La valutazione compiuta a priori sulla liceità del controllo potrebbe, infatti, risultare errata ove i dati non siano interpretati.
Di fatto, un controllo indiretto potrebbe configurarsi vietato a seguito dell'elaborazione dei dati acquisiti, in quanto volto a sorvegliare direttamente l'attività lavorativa o non risulti rispettoso del principio di proporzionalità.

Pensiamo, per esempio, agli *exhaust data.*
Come illustrato nel primo capitolo, questa tipologia di dati costituisce uno "scarto" delle operazioni svolte in ambienti digitali, la cui acquisizione può risultare (addirittura) sconosciuta e il cui significato è (in origine) ignoto.
Gli *exhaust data* possono, però, risultare utili alle organizzazioni per individuare l'esistenza di *pattern* di correlazione tra i lavoratori riscontrabili solo a seguito di analisi.
Pertanto, a seguito dell'interpretazione degli *exhaust data*, un controllo posto in essere per finalità organizzative-produttive potrebbe rivelare attitudini, preferenze e comportamenti di un lavoratore compiuti all'interno di un ambiente digitale, realizzando un monitoraggio diretto e sproporzionato dell'attività lavorativa.

La fase critica del controllo si sposterebbe, dunque, da quella di acquisizione dei dati a quella di elaborazione.
Ciò determina un possibile vuoto di tutela nella norma: un giudizio di legittimità del controllo compiuto su dati acquisiti apparentemente "neutri" (in quanto non significativi) potrebbe convertirsi in controllo "vessatorio" a seguito della loro interpretazione.
Solo mediante l'elaborazione è, infatti, possibile comprendere il significato delle informazioni assimilate e svolgere un'effettiva ponderazione sull'attinenza o meno dei dati registrati in relazione alla finalità di controllo condotta.

Lavoro, vol. II, n. 2, 2017, pp. 317 ss. Il GPDP in tale provvedimento ha affermato che: "*è illecita la registrazione in forma elettronica, da parte del datore di lavoro, delle attività di accesso ad internet e dell'utilizzo della posta elettronica dei lavoratori, effettuata tramite sistemi e apparecchiature differenti dalle ordinarie postazioni di lavoro, con modalità non percepibili dall'utente e indipendenti dalla normale attività lavorativa dell'utilizzatore, che si articoli in operazioni di controllo, filtraggio, monitoraggio e tracciatura massivi, prolungati, costanti ed indiscriminati delle connessioni internet, memorizzate in modo sistematico ed anelastico e conservate per un ampio arco temporale. Si tratta di strumenti idonei a consentire il controllo a distanza dell'attività dei lavoratori, in contrasto col divieto legislativo posto dalla disciplina tanto previgente quanto vigente, non potendo essere considerati strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa. Il relativo trattamento dei dati personali viola i principi di liceità e correttezza, di necessità, pertinenza e non eccedenza, e di proporzionalità, nonché l'obbligo di informativa degli interessati, con la conseguente inutilizzabilità dei dati*".

Spostare il momento di criticità del controllo alla fase di elaborazione porta a disgiungere due momenti: quello del monitoraggio e quello del controllo.
I termini "monitoraggio" e "controllo", spesso utilizzati quali sinonimi, acquisiscono ora un significato differente e tra loro complementare.
Il concetto di "monitoraggio" concerne propriamente la possibilità di guardare e ascoltare l'attività lavorativa che, nel caso di prestazioni "native digitali", avviene mediante la raccolta di dati prodotti dagli applicativi informatici.
Distintamente, il concetto di controllo "*evoca l'atto di esaminare qualcosa (l'attività dei lavoratori nella prospettiva dell'art. 4 SL) per verificare l'esattezza, la correttezza, la validità*"[253].
In questo senso, dunque, il termine monitoraggio "*può ricondursi ad un'attività che va oltre la dinamica dell'esercizio di un potere funzionale alla disciplina*"[254], ricomprendendo ogni operazione di raccolta delle informazioni "*idonea a partecipare al processo di determinazione delle misure organizzative*"[255].
Le potenzialità di "osservazione" e la sofisticata capacità di analizzare i dati scinderebbe, così, le due funzioni prima confuse.
Mentre è certa, infatti, la possibilità di monitorare ogni traccia digitale lasciata in ambienti virtuali, dubbio appare l'esercizio di un effettivo potere di controllo prima che i dati acquisiti siano resi comprensibili.
Davanti a informazioni che appaiono complesse e il cui significato è oscuro, ove non interpretato, nessuna attività di "attenta verifica" potrebbe essere utilmente esercitata.
Mentre per le prestazioni "analogiche" le fasi di "monitoraggio" e "controllo" coincidono, non essendoci bisogno di interpretare i dati, per le prestazioni "native digitali" la ponderazione *ex ante* sulla legittimità avverrà su elementi parziali, inidonei a valutare la vessatorietà del controllo.

Analizzare i dati può determinare, quindi, un "ampliamento" dello spettro di osservazione, portando a mutare la natura del controllo da preterintenzionale a diretto sulla prestazione.
In poche parole: elaborare dati dei lavoratori, per renderli significativi, potrebbe porre il datore di lavoro a esorbitare dal controllo oggettivo inizialmente dichiarato, offrendo uno sguardo privilegiato e diretto sull'attività del lavoratore.
Un controllo che sarebbe, così, vietato perché sproporzionato, pervasivo e occulto.

***

Alla luce di ciò, si intende analizzare una casistica delle condizioni di legittimità dei controlli a distanza svolti su prestazioni "native digitali" al fine di verificare se i limiti previsti all'esercizio del potere di controllo possano essere elusi a seguito dell'elaborazione dei dati acquisiti (in particolare ove "non autoevidenti").

La ricognizione, tenuto conto della complessità rimessa alle potenzialità di monitoraggio/elaborazione dei dispositivi tecnologici e alla varietà degli stessi, non potrà risultare esaustiva.

---

253 Stizia A., Lopez B., *Le più avanzate modalità di controllo sul lavoratore: Machine Learning e Social Media,* in Pisani C., Proia G., Topo A. (a cura di), *Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro*, Giuffrè Editore, Milano 2022, p. 366.
254 Stizia A., Lopez B., *Le più avanzate modalità di controllo sul lavoratore: Machine Learning e Social Media,* in Pisani C., Proia G., Topo A. (a cura di), *Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro*, Giuffrè Editore, Milano 2022, p. 366.
255Stizia A., Lopez B., *Le più avanzate modalità di controllo sul lavoratore: Machine Learning e Social Media,* in Pisani C., Proia G., Topo A. (a cura di), *Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro*, Giuffrè Editore, Milano 2022, p. 366.

Si esamineranno, quindi, le fattispecie che con maggior frequenza possono verificarsi nel contesto di una realtà aziendale dotata di strumenti informatici e digitali.
In particolare, per quanto riguarda le esigenze di organizzazione e produttive, si intende approfondire quanto attiene alla valutazione della *performance*.
In riferimento alla salute e sicurezza del lavoro, si analizzeranno gli studi che monitorano gli atteggiamenti e i comportamenti dei lavoratori in ambienti digitali, al fine di comprendere lo stato psico-fisico dei lavoratori, con particolare attenzione allo *stress* lavoro-correlato.
Infine, per quanto inerisce la tutela dal patrimonio aziendale, si farà riferimento al monitoraggio a cui è tenuto il datore di lavoro in qualità di Titolare del trattamento[256] e alle misure di sicurezza (organizzative e tecniche) che deve applicare ai sensi dell'art. 32 del GDPR[257].

2.3. Esigenze organizzative produttive: la valutazione della *performance*

Con l'espressione "controllo preterintenzionale" [258] si intendono quei controlli a distanza non diretti intenzionalmente a sorvegliare l'attività del lavoratore, ma compiuti in ragione di finalità giustificatrici, individuate dall'art. 4 SL, e diretti a soddisfare prerogative datoriali oggettive[259].
Il Legislatore ha, dunque, indicato i presupposti obiettivi che devono ricorrere perché gli strumenti di controllo possano essere installati.
La prima finalità indicata dall'art. 4 SL sono le esigenze organizzative e produttive tra cui rientra la valutazione della *performance*.
La valutazione non è un fenomeno nuovo nelle relazioni di lavoro.
I datori di lavoro, esercitando il potere direttivo, svolgono regolarmente un'attività di osservazione dei dipendenti trattandosi di un *facere* continuativo[260] che non si esaurisce in un'unica soluzione, perdurando per tutta la durata del rapporto contrattuale.
Tra i motivi legittimi per monitorare le prestazioni vi è quello di ottimizzare i processi organizzativi mediante tecniche di valutazione della *performance*.
La valutazione della *performance* può essere definita come la misurazione delle prestazioni svolte dalle risorse umane in relazione agli obiettivi manageriali, il cui risultato si quantifica in metriche che consentono di comprendere l'impatto dei risultati conseguiti in rapporto a quelli pianificati.
L'attività di valutazione è, dunque, intrinsecamente connessa a quella di misurazione.

La valutazione delle *performance* comporta un'analisi distinta rispetto ad un mero accertamento dell'esecuzione della prestazione, ovvero dell'adempimento dei compiti prescritti nel contratto di lavoro individuale e in quello collettivo di riferimento[261].

---

256 Art. 24 GDPR.
257 Per un approfondimento si rinvia al punto 2.5. del presente capitolo.
258 L'aggettivo "preterintenzionale", di derivazione penalista è utilizzato per definire un controllo mosso "al di là delle intenzioni", fa riferimento al controllo strumentale alle esigenze organizzative-produttive, di salute e sicurezza o tutela del patrimonio aziendale. Cfr. Del Punta R., *La nuova disciplina dei controlli a distanza sul lavoro (art. 23, d.lgs. n. 151/2015*), in *Rivista Italiana di Diritto del Lavoro (RIDL)*, vol. I, 2016, p. 78.
259 Cfr. Veneziani B., *Sub art. 4*, in Freni A. Giugni G. (diretto da), *Lo Statuto dei lavoratori. Commentario alla legge 20 maggio 1970, n. 300,* Giuffrè Editore, Milano, 1979, pp. 17 – 32.
260 Sulla questione si rinvia a Dessì O., *Il controllo a distanza sui lavoratori. Il nuovo art. 4 Stat. Lav.*, Edizioni Scientifiche Italiane, Napoli, 2017, pp. 16 – 17.
261 Ales E., *Is performance appraisal compatible with the employment relationship? A conclusive plea in favour of an achievement-oriented approach to work organization*, in Addabbo T., Ales E., Curzi Y., Fabbri T., Rymkevich O., Senatori I. (eds.), *Performance Appraisal in Modern Employment Relations. An Interdisciplinary Approach*, Palgrave Macmillan, Cham, 2020.

Stimare una *performance* implica un giudizio su differenti attitudini e capacità del singolo quali possono essere la formazione, le interazioni e i comportamenti tenuti con i colleghi, il coinvolgimento e l'attaccamento all'organizzazione, la soddisfazione o lo *stress* connesso ai propri compiti.
Comprendere gli atteggiamenti dei lavoratori consente di interpretare la percezione che questi hanno dell'organizzazione e come la stessa influisca sul loro operato, così da adeguare i modelli di gestione vigenti.
Valutare la *performance* permette, inoltre, di intraprendere azioni di valorizzazione dei comportamenti umani per il conseguimento il più possibile efficiente degli scopi prefissati.
Se è vero, infatti, che *"le persone formano il posto di lavoro*"[262] tale affermazione acquisisce una rilevanza ancora maggiore a seguito della digitalizzazione che, dematerializzando il lavoro, ha posto le risorse umane al centro del processo decisionale.
Capire le percezioni dei lavoratori, in quanto modellatori del comportamento, diviene elemento di sviluppo e competitività per le imprese e per la loro organizzazione.
L'interesse dei datori di lavoro per la valutazione della *performance* sembra, dunque, spostare il *focus* del controllo dalla diligenza al valore del risultato della prestazione, tradizionalmente estranea alla struttura dell'obbligazione lavorativa[263].
Interpretare i comportamenti e le attitudini è, tuttavia, un compito complesso.
Il vaglio di tali elementi si avvale tradizionalmente di strumenti quali questionari, colloqui e osservazione diretta dei lavoratori.
Queste tecniche trovano, però, il proprio limite nella soggettività riscontrabile nel valutatore, a cui è rimessa l'osservazione e l'interpretazione degli elementi di indagine, e nei valutati, influenzati dalla propria emotività oppure portati a mentire[264] per conformarsi alle aspettative datoriale o tutelare la propria *privacy*.
Gli errori più frequenti possono essere ricondotti a processi cognitivi legati alla rappresentatività (che porta ad assumere decisioni considerando solo caratteristiche parziali dell'individuo), al processo selettivo e valutativo delle informazioni acquisite, nonché all'ancoraggio a pregiudizi o stereotipi.
Ciò determina un giudizio soggettivo, non strutturato o rigoroso, e, pertanto, non affidabile[265].
Tali indagini richiedono, inoltre, risorse e tempo che inibiscono la capacità di elaborare modelli efficaci e tempestivi[266] alle necessità imprenditoriali.
Con la digitalizzazione del lavoro la valutazione della *performance* ha innovato le proprie tecniche mediante l'utilizzo di nuovi *output*: i dati che codificano le prestazioni.
L'uso di piattaforme o l'implementazione della tecnologia negli uffici "intelligenti"[267], generano spazi di evoluzione dinamica destinanti a potenziare la connessione e la collaborazione tra i lavoratori.
Diretta conseguenza di ciò è la possibilità di osservare con maggiore precisione le interazioni e di acquisire informazioni sulle correlazioni.

---

262 Schneider B., *The people make the place*, in *Personnel Psychology*, vol. 40, n. 3, 1987, 437–453.
263 Cfr. Ingrao A. *Il controllo a distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata*, Cacucci Editore, Bari, 2018, p.180.
264 Florczak I., Wujczyk M., *The lie as a privacy protection measure*, in Addabbo T., Ales E., Curzi Y., Fabbri T., Rymkevich O., Senatori I., *Performance appraisal in modern employment relations. An interdisciplinary approach*, Palgrave Macmillan, Switzerland, 2020, pp.137 – 164.
265 Cherry M. A., *People Analytics and invisible labor*, in *Saint Louis University Law Journal*, vol. 61, n. 1, 2016, p. 8.
266 Cfr. Gelbard R., Ramon-Gonen R., Carmeli A., Bittmann R. M., Talyansky R, *Sentiment analysis in organizational work: Towards an ontology of people analytics,* in *Wiley Expert Systems*, 2018, pp. 1- 15.
267 Per esempio, mediante l'utilizzo di assistenti vocali come Amazon Alexa, dispositivi *Internet of Things (IoT),* interconnessi mediante *internet* e capaci di fornire un supporto all'attività lavorativa. Cfr. Bogdan R., Tatu A., Crisan-Vida M. M., Popa M., Stoicu-Tivadar L., *A practical experience on the Amazon Alexa integration in smart offices*, in Sensors, vol. 21, n. 734, 2021, pp. 1- 21.

La digitalizzazione del lavoro rende, infatti, *in re ipsa* analizzabile la prestazione svolta mediante dispositivi tecnologici e, contemporaneamente, intrinsecamente necessario il monitoraggio, quando viene meno la presenza fisica dei lavoratori.
In tale prospettiva si è osservata la progressiva adozione di *Enterprise Collaborative Software* (ECS)[268] da parte di grandi imprese, il cui utilizzo favorisce l'interazione tra i dipendenti e, contemporaneamente, l'acquisizione di informazioni sotto forma di tracce digitali.
L'osservazione del lavoro digitale consente di svolgere, dunque, una doppia valutazione: quella tradizionale (certamente più accurata grazie al supporto tecnologico) ed una innovativa (basata sui dati).
La valutazione della *performance* basata sui dati permette, inoltre, di ricercare elementi caratterizzanti i "comportamenti innovativi"[269].
La digitalizzazione del lavoro, infatti, non ha solo modificato i metodi valutativi, ma ha anche individuato nuovi obiettivi di *management* meritevoli di essere conseguiti.
La capacità dei lavoratori di essere innovativi è considerata una competenza chiave soprattutto negli ambienti digitali, divenendo un obiettivo organizzativo e, in quanto tale, oggetto di valutazione della *performance*.
Le risorse umane possono, così, influenzare lo sviluppo e la competitività di un'impresa mediante l'esecuzione di "comportamenti lavorativi innovativi" (*innovative work behavior – IWB*) consistenti in attività propositive, capaci di generare e diffondere idee, ultronee rispetto all'esecuzione della mera prestazione contrattuale[270].
L'analisi di comportamenti innovativi è posta in essere da aziende primarie nel settore tecnologico quali Google che, attraverso un'attenta valutazione degli atteggiamenti e percezioni dei dipendenti, ha ottenuto un rilevante sviluppo - anche di *business* - tanto da istituire il "*People & Innovation Lab*" che con il "*Project Oxygen*"[271] ha definito le caratteristiche dei propri "*top manager*". Il progetto ha attuato una dettagliata analisi qualitativa dei responsabili in forza, correlando elogi e reclami ricevuti, aspettative e obiettivi conseguiti, frasi e interlocuzioni utilizzate dai soggetti valutati.
La digitalizzazione del lavoro condiziona anche i criteri di valutazione, determinando l'esigenza di definire nuovi *benchmark,* non essendo più attuali quelli basati su una metrica spazio-temporale definiti per un lavoro in presenza.
Analizzare la *performance* con *standard* adottati nel 1919 dall'Organizzazione Internazionale del Lavoro (OIL)[272], presuppone una modalità di esecuzione profondamente diversa, improntata su una giornata lavorativa di otto ore trascorse nell'adempimento di attività manuali, in cui la collaborazione tra lavoratori non costituisce elemento di valore e l'innovazione non rappresenta un requisito di competitività.

---

[268] T. Fabbri, F. Mandreoli, R. Martoglia, A. C. Scapolan, *Employee Attitudes and (Digital) Collaboration Data: A Preliminary Analysis in the HRM Field*, 28th International Conference on Computer Communication and Networks (ICCCN), n. 7, 2019, p.1-6. This work is supported by UniMoRe under the project "*Framing employee attitudes and digital work behaviors to support data-driven human resource management.*

[269] Curzi Y., Fabbri T. e Pistoresi B., *Performance appraisal criteria and innovative work behaviour: the mediati grole of employees' appraisal satisfaction*, in Addabbo T., Ales E., Curzi Y., Fabbri T., Rymkevich O., Senatori I. (eds.), *Performance Appraisal in Modern Employment Relations. An Interdisciplinary Approach*, Palgrave Macmillan, Cham, 2020.

[270] Cfr Curzi Y., Fabbri T., Scapolan A. C., Boscolo S., *Performance appraisal and innovative behavior in digital era*, in *Frontiers in Psycology,* Vol. 10, July 2019, pp. 1-12.

[271] Shrivastava S., Nagdev K., Rajesh A., *Redefining HR using people analytics: the case of Google,* in *Human Resource Management International Digest,* vol. 26, n. 2, 2018, p. 4. Il Progetto prevedeva l'individuazione dei "*top manager*" capaci di stimolare l'insorgere di "comportamenti innovativi" tramite l'analisi delle valutazioni ricevute dai sottoposti, delle parole utilizzate in testi e discorsi oltre che il conseguimento di obiettivi. L'individuazione dei "*top manager*" è stata, dunque, svolta su un sistema di analisi "misto" includendo valutazione della *performance*, *Sentiment Analysis* e analisi del testo. I risultati hanno poi portato alla predisposizione di percorsi formativi per i manager di Google al fine di adeguarli agli *standard* di "*top manager*" individuati.

[272] International Labour Organization (ILO), *Interpretation of a decision concerning the Hours of Work (Industry), Convention, 1919 n. 1.*

L'adeguamento dei modelli non può tradursi in una valutazione per obiettivi, non potendo ricondurre ogni prestazione digitale a un risultato da conseguire.
La necessità di un aggiornamento dei *benchmark* di valutazione è stata rilevato anche dalle Parti Sociali, le quali, comprendendo che non tutte le attività etero-organizzate possono essere valutate in relazione ad un *target*, hanno distinto il "lavoro agile giornaliero", applicato ad "*ambiti organizzativi caratterizzati da attività svolte per obiettivi con adeguato livello di autonomia e flessibilità oraria*" [273], dal "lavoro agile settimanale" valido per "*ambiti organizzativi nei quali le attività svolte sono etero organizzate, non consentono di organizzare il lavoro per obiettivi e per i quali è indispensabile garantire il presidio in specifici archi orari*"[274].
I nuovi *benchmark* di valutazione potrebbero essere definiti proprio con tecniche di analisi dei dati, tenendo in considerazione le nuove prerogative richieste dall'innovazione.
La valutazione della *performance*, attraverso l'utilizzo di tecniche analitiche di *data mining* cerca, pertanto, di porre rimedio alle criticità riscontrate nell'analisi tradizionale nonché di sfruttare le potenzialità dei dati per individuare "*soft skill*"[275] e fattori di "lavoro invisibile"[276] che caratterizzano l'innovatività[277].
Tale opportunità è una nuova potenzialità di indagine basata sull'evidenza di elementi empirici che permette di valutare in modo imparziale l'adempimento della prestazione e della *performance*.
La datificazione[278] del lavoro consente, dunque, di rilevare senza interposizioni i tradizionali elementi di *performance* attraverso nuove manifestazioni. Per esempio, l'attaccamento ad una realtà imprenditoriale di un dipendente può essere interpretato mediante le interazioni compiute sulla piattaforma di lavoro con i colleghi.
L'analisi compiuta con i dati supporta, inoltre, l'organizzazione aiutando a comprendere atteggiamenti non rilevabili direttamente, fornendo un'interpretazione delle correlazioni, eliminando la soggettività dal processo valutativo e fornendo risposte tempestive alle contingenti esigenze manageriali.

Nell'ordinamento italiano i sistemi di valutazione della *performance* per il lavoro privato sono svincolati da norme, diversamente da quanto avviene nel settore pubblico[279].
Il concetto di valutazione della *performance* viene richiamato, per esempio, in relazione alle "posizioni organizzative"[280]. Il termine "posizioni organizzative" fa riferimento a quelle figure professionali, poste

---

273 Art. 15 Accordo Tim sullo *smart working* del 4 Agosto 2020.
274 Art. 16 Accordo Tim sullo *smart working* del 4 Agosto 2020.
275 Con il concetto di *soft skill* si comprendono le qualità personali delle persone, l'approccio che queste manifestano nelle relazioni interpersonali, l'atteggiamento espressi in relazione con l'ambiente con cui interagisce e le modalità attraverso le quali vengono affrontati i problemi. Le *soft skill* sono, dunque, tutte le attitudini e qualità che compongono la sfera individuale di un soggetto e che ne determina l'agire e la predisposizione o predilezione per un determinato comportamento. Cfr. Grugulis I., Vincent S., *Whose skill is it anyway? 'Soft' skills and polarization,* in *Work Employ*ment & Society, vol. 23, n. 4, 2009, pp.597–615.
276 Per "lavoro invisibile" si intende l'attività che si verifica nel contesto del lavoro subordinato e che i lavoratori svolgono in risposta ai requisiti (impliciti o espliciti) dei datori di lavoro ed è fondamentale per generare reddito, ottenere o mantenere i posti di lavoro e per promuovere la carriera. In merito Cherry M. A., *People Analytics and invisible labor*, in *Saint Louis University Law Journal*, vol. 61, n. 1, 2016, pp. 1 – 16.
277 Sul tema anche E. Dagnino, *Dalla fisica all'algoritmo: una prospettiva di analisi giuslavoristica*, ADAPT University Press, 2019.
278 Bertolli F., Fabbri T., Mandreoli F., Martoglia R., Scapolan A.C., *Work datafication and digital work behavioranalysis as a source of social good,* Conference Paper 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC).
279 Le Pubbliche Amministrazioni devono, per Legge, valutare le proprie *performance* in forza di quanto previsto dal D. Lgs. 150/2009, la cosiddetta "*Legge Brunetta*", che all'art.3 comma 2 statuisce che "*ogni amministrazione pubblica è tenuta a misurare e a valutare la performance con riferimento all'amministrazione nel suo complesso, alle unità organizzative o aree di responsabilità in cui si articola e ai singoli dipendenti*". La norma, da ultimo modificata con il D. Lgs 74/2017, è la conclusione di un percorso iniziato nel ventennio precedente che ha gradualmente introdotto nella gestione della Pubblica Amministrazione criteri aziendalistici e manageriali.
280 Previste inizialmente dall'art. 45 comma 3 del D. Lgs. 3 febbraio 1993 n. 29 "*Razionalizzazione dell'organizzazione delle amministrazioni pubbliche e revisione della disciplina in materia di pubblico impiego, a norma dell'art. 2 della legge 23 ottobre 1992, n. 421*) rubricato "*Contratti collettivi nazionali e integrativi*" prevede che "*mediante appositi accordi tra l'ARAN e le confederazioni rappresentative ai sensi dell'articolo 47-bis, comma 4, sono stabiliti i comparti della contrattazione collettiva nazionale riguardanti settori omogenei o affini. I dirigenti costituiscono un'area contrattuale autonoma relativamente a uno o più comparti. Resta fermo per l'area contrattuale della dirigenza del ruolo sanitario quanto previsto dall'art. 15 del D.Lgs. 30 dicembre 1992 n. 502 e successive modifiche. Agli*

in posizioni di elevata responsabilità che svolgono compiti direzionali o che comportano iscrizioni ad albi o dotate di peculiari caratteristiche tecnico-scientifiche.
Secondo l'interpretazione della Suprema Corte[281], il conferimento di una posizione organizzativa costituisce un'attribuzione temporanea di una posizione di responsabilità e non l'inquadramento in una nuova categoria contrattuale.
La posizione organizzativa può, dunque, venire meno qualora non sia rispettata la *performance* attesa in ragione dell'incarico affidato.
A riguardo, il CCNL del 21 maggio 2018 delle Autonomie locali, prevede che questa possa cessare "*(…) in conseguenza di valutazione negativa della performance individuale"* (art. 14 comma 3).
Traspare, dunque, come l'organizzazione aziendale (anche nel caso di un'impresa pubblica) sia strettamente connessa alla valutazione delle *performance*[282].

Mancando, quindi, una precisa regolamentazione nel settore privato, la definizione e i limiti di cosa sia valutabile ai fini della "*performance*" sono rimessi alla contrattazione collettiva e alla giurisprudenza.
L'indagine svolta dalla Giurisprudenza italiana, sia di merito che di legittimità, si è concentrata soprattutto sul concetto di "*scarso rendimento*"[283] al fine di determinare quando l'esecuzione di una prestazione "non performante" sia riconducibile al concetto di "inadempimento punibile" a fini disciplinari[284].
La ricerca giurisprudenziale relativa allo scarso rendimento ha altresì interessato il trasferimento per esigenze produttive, come disciplinato dall'art. 2103 c.c.
La stessa Corte di Cassazione ha ritenuto che: "l*egittimamente, in caso di trasferimento, il datore di lavoro attribuisce rilevanza a situazioni soggettive, nella specie, scarso rendimento del dipendente, laddove ciò avvenga non con intenti punitivi, ma secondo il criterio obiettivo della funzionalità dell'organizzazione*"[285].
Viene, dunque, riconosciuto al datore di lavoro il potere organizzativo di risolvere problemi connessi ad una prestazione "non performante", sindacabile solo in quanto discriminatoria o lesiva del criterio di ragionevolezza.
Nessuna pronuncia si è, tuttavia, ancora espressa in merito alla valutazione della *performance* mediante tecniche di *data mining.*
La contrattazione collettiva, d'altro canto, non ha fornito risposte univoche in merito a cosa sia misurabile e come debba essere eseguita la valutazione mediante il supporto di dati.

---

accordi che definiscono i comparti o le aree contrattuali si applicano le procedure di cui all'articolo 46, comma 5. Per le figure professionali che, in posizione di elevata responsabilità, volgono compiti di direzione o che comportano iscrizione ad albi oppure tecnico scientifici e di ricerca, sono stabilite discipline distinte nell'ambito dei contratti collettivi di comparto".

281 Cfr. Corte di Cassazione, sez. lav. ordinanza del 10.07.2019 n. 18561.

282 A riguardo la giurisprudenza di merito ha sottolineato come non sussiste un diritto soggettivo del pubblico dipendente ad essere preposto ad una posizione organizzativa, neppure nel caso in cui questi l'abbia già ricoperta in forza di un precedente incarico, trattandosi di scelta ascrivibile al potere organizzativo dell'ente basata anche sulla valutazione della performance ottenuta. Da ciò, deriva il carattere fiduciario e temporaneo dell'incarico. A riguardo Corte App. Firenze del 28.01.2005; Trib. di Caltanissetta del 14.01.2006; Trib. di Bari del 22.05.2014.

283 Viceconte M.*, Lo scarso rendimento nel rapporto di lavoro subordinato,* nota a sentenza alla C. Cass. sez. Lavoro ordinanza del 08.05.2018 n. 10963 in Giurisprudenza Italiana, n.7, 2018.

284 La Suprema Corte ha delineato chiaramente i confini dell' inadempimento punibile, seppure in una fattispecie di licenziamento, ed ha rilevato che "*nel contratto di lavoro subordinato, il lavoratore non si obbliga al raggiungimento di un risultato ma alla messa a disposizione del datore delle proprie energie, nei modi e nei tempi stabiliti, con la conseguenza che il mancato raggiungimento del risultato prefissato non costituisce di per sé inadempimento, giacché si tratta di lavoro subordinato e non dell' obbligazione di compiere un' opera o un servizio (lavoro autonomo). Ove, tuttavia, siano individuabili dei parametri per accertare che la prestazione sia eseguita con la diligenza e professionalità medie, proprie delle mansioni affidate al lavoratore, il discostamento dai detti parametri può costituire segno o indice di non esatta esecuzione della prestazione*" (Corte di Cass. 8973/91 richiamata dalla sentenza della Corte di Cass. 23735/2016). In tal senso anche Tribunale di Trieste sez. lav. sent. 175/2019.

285 Si veda Corte di Cass. Civ. Sez. lav. n.11339/92.

Un riferimento si ritrova nella sezione "innovazioni tecnologiche" dell'Accordo quadro per le Telecomunicazioni del 21 febbraio 2019 ove viene prevista la definizione di linee guida, da inserire nel CCNL Telecomunicazioni, "*utili ad agevolare la diffusione di intese aziendali disciplinanti l'utilizzo ai fini organizzativi e produttivi dei dati relativi alle prestazioni lavorative, per la reportistica, il monitoraggio e il controllo dei livelli di servizio, nonché per l'analisi del contatto*".
Previsione attuata all'art. 57 del CCNL Telecomunicazioni rinnovato il 12.11.2020 rubricato "nuove tecnologie e tutela dei diritti dei lavoratori" in cui viene fatto riferimento "*all'utilizzo di sistemi, anche basati su modelli di Intelligenza Artificiale, finalizzati a verificare le performance qualitative e sui (…) servizi resi (…) ed accrescere la qualità del servizio attraverso la valorizzazione delle competenze professionali supportate anche da idonei percorsi formativi (…)*" nonché "*all'analisi sui dati generati dai sistemi, anche basati su modelli di Intelligenza Artificiale per finalità di tipo statistico (…) mirate alla valutazione e al miglioramento del livello di servizio offerto alla clientele nonché per l'analisi della qualità del servizio erogato (…)*".
Una concreta definizione sull'acquisizione e utilizzo dei dati ai fini della valutazione della *performance* è, però, assente all'interno del Contratto collettivo citato. Le Parti Sociali hanno, tuttavia, iniziato a comprendere la crescente rilevanza dell'impiego dei dati.
Anche il rinnovato CCNL Metalmeccanici del 5 febbraio 2021, nel disciplinare il Lavoro Agile, non entra nello specifico delle modalità di valutazione della *performance*. Il contratto collettivo rimette ad una Commissione Nazionale[286] paritetica il compito di definire una cornice contrattuale di riferimento su alcune tematiche che caratterizzano lo *smart working* quali il diritto alla disconnessione, la tutela della *privacy* e l'impiego di strumenti di lavoro informatici.
Mancano, però, riferimenti sull'utilizzo dei dati anche a fini valutativi.
Nessuna indicazione viene fornita in merito anche dal recente Protocollo Nazionale sul lavoro in modalità agile nel settore privato del 7 dicembre 2021.

Quello che certamente si può affermare è che la valutazione delle *performance* sta variando contestualmente alla digitalizzazione del lavoro, passando da un monitoraggio diretto dei dipendenti a tecnologie innovative, quali possono essere le *People Analytics*, che sfruttano i dati per compiere le proprie analisi.

***

Al temine della disamina su cosa sia una valutazione della *performance* e come questa sia variata in ragione della digitalizzazione del lavoro ci si chiede se, attraverso l'analisi dei dati, il controllo potrebbe esorbitare l'ambito dell'esigenza organizzativa-produttiva rivelandosi capace di controllare direttamente i lavoratori nello svolgimento della loro attività.
Il quesito coinvolge, quindi, la capacità di eseguire a priori un giudizio sulla fondatezza della finalità di valutazione della *performance* sulla base dei dati conosciuti o conoscibili prima della loro elaborazione.
Osservare dati acquisiti da *Digital Workplace* e impiegarli per compiere una valutazione della *performance* è, infatti, una circostanza differente dal visionare dati "autoevidenti" registrati in un ambiente analogico.
I dati afferenti ad un ambiente di lavoro "fisico" riportano informazioni immediatamente comprensibili che permettono di ponderare correttamente se le informazioni acquisite rispondono alle finalità produttive-organizzative o eccedono tale scopo.
Differentemente, acquisire dati "non autoevidenti" porta a svolgere una stima "alla cieca" in riferimento all'attinenza o meno delle informazioni registrate.
Solo a seguito dell'elaborazione dei dati questi disveleranno il loro reale significato e valore.

[286] La commissione si è insediata il 10 maggio 2021.

Tale situazione può determinare un'erronea valutazione in merito ai dati registrati: una volta interpretati questi potrebbero restituire informazioni ultronee rispetto alla finalità dichiarata.

Valutare la *performance* di attività "native digitali" potrebbe, quindi, consentire un controllo sproporzionato o diretto dell'attività lavorativa.
Per esempio, nel caso in cui la valutazione della *performance* interessi anche degli "*exhaust data*", ovvero gli "scarti" delle operazioni compiute in un ambiente digitale, l'analisi potrebbe restituire informazioni molto dettagliate sulle prestazioni espletate e sulle interazioni intrattenute dagli utenti.
Informazioni che realizzerebbero (di fatto) un controllo diretto del lavoratore o, comunque, sproporzionato rispetto all'esigenza giustificatrice del controllo.
Gli stessi "metadati", però, prima di un intervento interpretativo risulterebbero "neutri", ovvero trasparenti alla finalità organizzativa-produttiva perseguita e privi di rilevanza in riferimento al divieto di cui al comma 1 dell'art. 4 SL.
Anzi, proprio la loro natura di "scarti" potrebbe rendere inizialmente ignoto non solo il loro significato, ma anche il possesso da parte del datore di lavoro.

Il giudizio di legittimità sul controllo posto in essere per fini valutativi della *performance* potrebbe, così, risultare fallace.

La finalità organizzativa-produttiva in un contesto di prestazioni "native digitali" può, quindi, consentire di svolgere analisi sofisticate su dati apparentemente privi di importanza, ma inidonei a fornire una sorveglianza accurata delle attività e dei comportamenti dei lavoratori.
Al pari di quanto si avrà modo di illustrare nel punto seguente, un ulteriore rischio connesso all'impiego di tecniche di *Data Analysis* è quello di eseguire una profilazione dei dipendenti, tracciando minuziosamente aspetti professionali e personali.
La fase critica del controllo passa, dunque, dal momento dell'acquisizione a quello dell'elaborazione dei dati che consente, in taluni casi, di eseguire un controllo sproporzionato o diretto sotto un'apparente "scudo" di legittimità. La finalità giustificatrice di un controllo "preterintenzionale", può, infatti, essere travalicata nel momento in cui i dati vengono interpretati.

2.4. Esigenze di salute e sicurezza sul lavoro: la valutazione dei rischi da iperconnessione

La tutela della salute e sicurezza dei lavoratori è una delle esigenze previste dalla norma statutaria per cui è ammesso il controllo a distanza da parte del datore di lavoro ai sensi dell'art. 4 comma 1.
La nozione di "sicurezza sul lavoro" coinvolge l'insieme delle misure tecnico organizzative, medico sanitarie, formative, procedurali finalizzate alla prevenzione di eventi di danno nei confronti dei lavoratori durante lo svolgimento dell'attività lavorativa.
La tutela prevenzionistica trova fondamento nell'art. 32 della Costituzione e nell'art. 2087 C.c. che costituisce la fonte della responsabilità datoriale.
La norma da ultimo citata prevede, infatti, che "*l'imprenditore è tenuto ad adottare nell'esercizio dell'impresa le misure che, secondo la particolarità del lavoro, l'esperienza e la tecnica, sono necessarie a tutelare l'integrità fisica e la personalità morale dei prestatori di lavoro*".
Alla base vi è la responsabilità del datore di lavoro per rischio professionale (ex art. 9 SL e art. 2087 C.c.), il quale presuppone un criterio di imputazione oggettivo per i danni eventualmente patiti dai lavoratori[287].

[287] Di qui deriva "*l'obbligatorietà di un peculiare schema assicurativo con l'INAIL per il datore di lavoro che, al verificarsi dell'evento, permette di erogare una prestazione previdenziale ai lavoratori: la tutela è riconosciuta soltanto a alcuni lavoratori che sono esposti a certi rischi; non è garantita*

La disposizione impone, quindi, al datore di lavoro l'obbligo di adottare le misure che, secondo la particolarità del lavoro, l'esperienza e la tecnica, sono necessarie a tutelare l'integrità fisica e la personalità morale dei lavoratori che possono derivare da fattori esterni al luogo di lavoro durante lo svolgimento della prestazione[288].

Gli obblighi specifici vigenti in capo al datore di lavoro sono individuati dal D. Lgs. 81/2008 (T.U. sulla salute e sicurezza sul lavoro) all'art. 18 rubricato "*Obblighi del datore di lavoro e del dirigente*"[289].

Anche in ambito prevenzionistico l'utilizzo di tecnologia abilitante introdotta dall'Industria 4.0 ha apportato significative potenzialità da un punto di vista del supporto ai lavoratori e nelle possibilità di diversificare i fattori di rischio attraverso il monitoraggio dell'ambiente di lavoro e dell'attività dei lavoratori.

---

l'equivalenza tra prestazione economica e entità del danno (c'è, infatti, un indennizzo, non un risarcimento del danno); l'assicurazione può non coprire tutti i danni e non interviene nei casi meno gravi (lesioni lievi)". Così Faioli M., *Data analytics, robot intelligenti e regolazione del lavoro*, in *Federalismi.it*, n. 9, 2022, p.160.

288 In merito Corte di Cass n. 24742 dell'8.10.2018; Corte di Cass. n. 13956 del 3.8.2012.

289 Art. 18 D.Lgs. 81/2008*: "1. Il datore di lavoro, che esercita le attività di cui all'articolo 3, e i dirigenti, che organizzano e dirigono le stesse attività secondo le attribuzioni e competenze ad essi conferite, devono: a) nominare il medico competente per l'effettuazione della sorveglianza sanitaria nei casi previsti dal presente decreto legislativo. b) designare preventivamente i lavoratori incaricati dell'attuazione delle misure di prevenzione incendi e lotta antincendio, di evacuazione dei luoghi di lavoro in caso di pericolo grave e immediato, di salvataggio, di primo soccorso e, comunque, di gestione dell'emergenza; c) nell'affidare i compiti ai lavoratori, tenere conto delle capacità e delle condizioni degli stessi in rapporto alla loro salute e alla sicurezza; d) fornire ai lavoratori i necessari e idonei dispositivi di protezione individuale, sentito il responsabile del servizio di prevenzione e protezione e il medico competente, ove presente; e) prendere le misure appropriate affinché soltanto i lavoratori che hanno ricevuto adeguate istruzioni e specifico addestramento accedano alle zone che li espongono ad un rischio grave e specifico; f) richiedere l'osservanza da parte dei singoli lavoratori delle norme vigenti, nonché delle disposizioni aziendali in materia di sicurezza e di igiene del lavoro e di uso dei mezzi di protezione collettivi e dei dispositivi di protezione individuali messi a loro disposizione; g) richiedere al medico competente l'osservanza degli obblighi previsti a suo carico nel presente decreto; h) adottare le misure per il controllo delle situazioni di rischio in caso di emergenza e dare istruzioni affinché i lavoratori, in caso di pericolo grave, immediato ed inevitabile, abbandonino il posto di lavoro o la zona pericolosa; i) informare il più presto possibile i lavoratori esposti al rischio di un pericolo grave e immediato circa il rischio stesso e le disposizioni prese o da prendere in materia di protezione; l) adempiere agli obblighi di informazione, formazione e addestramento di cui agli articoli 36 e 37; m) astenersi, salvo eccezione debitamente motivata da esigenze di tutela della salute e sicurezza, dal richiedere ai lavoratori di riprendere la loro attività in una situazione di lavoro in cui persiste un pericolo grave e immediato; n) consentire ai lavoratori di verificare, mediante il rappresentante dei lavoratori per la sicurezza, l'applicazione delle misure di sicurezza e di protezione della salute; o) consegnare tempestivamente al rappresentante dei lavoratori per la sicurezza, su richiesta di questi e per l'espletamento della sua funzione, copia del documento di cui all'articolo 17, comma 1, lettera a), nonché consentire al medesimo rappresentante di accedere ai dati di cui alla lettera r); p) elaborare il documento di cui all'articolo 26, comma 3, e, su richiesta di questi e per l'espletamento della sua funzione, consegnarne tempestivamente copia ai rappresentanti dei lavoratori per la sicurezza; q) prendere appropriati provvedimenti per evitare che le misure tecniche adottate possano causare rischi per la salute della popolazione o deteriorare l'ambiente esterno verificando periodicamente la perdurante assenza di rischio; r) comunicare all'INAIL, o all'IPSEMA, in relazione alle rispettive competenze, a fini statistici e informativi, i dati relativi agli infortuni sul lavoro che comportino un'assenza dal lavoro di almeno un giorno, escluso quello dell'evento e, a fini assicurativi, le informazioni relative agli infortuni sul lavoro che comportino un'assenza dal lavoro superiore a tre giorni; s) consultare il rappresentante dei lavoratori per la sicurezza nelle ipotesi di cui all'articolo 50; t) adottare le misure necessarie ai fini della prevenzione incendi e dell'evacuazione dei luoghi di lavoro, nonché per il caso di pericolo grave e immediato, secondo le disposizioni di cui all'articolo 43. Tali misure devono essere adeguate alla natura dell'attività, alle dimensioni dell'azienda o dell'unità produttiva, e al numero delle persone presenti; u) nell'ambito dello svolgimento di attività in regime di appalto e di subappalto, munire i lavoratori di apposita tessera di riconoscimento, corredata di fotografia, contenente le generalità del lavoratore e l'indicazione del datore di lavoro; v) nelle unità produttive con più di 15 lavoratori, convocare la riunione periodica di cui all'articolo 35; z) aggiornare le misure di prevenzione in relazione ai mutamenti organizzativi e produttivi che hanno rilevanza ai fini della salute e sicurezza del lavoro, o in relazione al grado di evoluzione della tecnica della prevenzione e della protezione; aa) comunicare annualmente all'INAIL i nominativi dei rappresentanti dei lavoratori per la sicurezza; bb) vigilare affinché i lavoratori per i quali vige l'obbligo di sorveglianza sanitaria non siano adibiti alla mansione lavorativa specifica senza il prescritto giudizio di idoneità. 2. Il datore di lavoro fornisce al servizio di prevenzione e protezione ed al medico competente informazioni in merito a: a) la natura dei rischi; b) l'organizzazione del lavoro, la programmazione e l'attuazione delle misure preventive e protettive; c) la descrizione degli impianti e dei processi produttivi; d) i dati di cui al comma 1, lettera r), e quelli relativi alle malattie professionali; e) i provvedimenti adottati dagli organi di vigilanza. 3. Gli obblighi relativi agli interventi strutturali e di manutenzione necessari per assicurare, ai sensi del presente decreto legislativo, la sicurezza dei locali e degli edifici assegnati in uso a pubbliche amministrazioni o a pubblici uffici, ivi comprese le istituzioni scolastiche ed educative, restano a carico dell'amministrazione tenuta, per effetto di norme o convenzioni, alla loro fornitura e manutenzione. In tale caso gli obblighi previsti dal presente decreto legislativo, relativamente ai predetti interventi, si intendono assolti, da parte dei dirigenti o funzionari preposti agli uffici interessati, con la richiesta del loro adempimento all'amministrazione competente o al soggetto che ne ha l'obbligo giuridico".*

In riferimento alle prestazioni "analogiche", i dispositivi dotati di servizio IOT (*Internet of things)*[290] hanno permesso di fornire un ampio supporto nell'ambito della salute e sicurezza dei lavoratori.
Il termine IOT viene utilizzato nel contesto odierno per indicare quegli oggetti che interagiscono e cooperano tra loro mediante connessione di rete. Oltre che con *pc* e *smartphone*, le interazioni possono interessare dispositivi indossabili (*wearable device*), di automazione o assistenza (come avviene con le *smart cars*).
Un dispositivo IOT, in quanto dotato di *hardware, software* e reti di comunicazione, può connettersi ad altri strumenti, generando un flusso continuo di dati fra utente e fornitore del servizio che, nelle relazioni lavorali, si identificano in dipendenti e datori di lavoro.
L'adozione di tecnologie dotate di servizio IOT in ambito di salute e sicurezza permette, quindi, un'attività di monitoraggio che può essere categorizzata a seconda che il controllo abbia ad oggetto condizioni esterne rispetto al lavoratore (non utilizzando dati personali) oppure che riguardi direttamente i lavoratori (facendo uso di dati personali)[291].
Le potenzialità di un servizio IOT si possono apprezzare soprattutto nel caso di un monitoraggio "diretto" dei lavoratori mediante l'impiego di dispositivi indossabili denominati *wearable device*[292]. Tali strumenti sono utilizzati da imprese, come ENI, per monitorare lo stato di salute dei propri dipendenti al fine di supportarne la sicurezza nello svolgimento dell'attività lavorativa.
La società citata, congiuntamente al *Mobile Experience Lab* del MIT di Boston, ha progettato e integrato presso le proprie raffinerie una linea di indumenti e accessori *smart* dotati di biosensori capaci di misurare frequenza cardiaca, respirazione, sudorazione e posizione assunta dal lavoratore[293].
Tali strumenti svolgono un monitoraggio costante dei parametri inerenti allo stato di salute dei lavoratori, al fine di vigilare le condizioni di prestatori potenzialmente esposti a situazioni di pericolo sulle piattaforme.
Il supporto fornito dai *wearable device* e la potenzialità di elaborare i dati (dagli stessi registrati) offrono un servizio di grande utilità nel processo di individuazione di eventuali rischi per la salute e nella gestione degli stessi.
In un'ottica di prevenzione e protezione, pertanto, poter monitorare questi parametri consente di migliorare gli *standard* di intervento e di provvedere tempestivamente nel caso del verificarsi di specifici fattori di rischio sulla base delle esigenze di ogni singolo lavoratore.
L'acquisizione di questi dati implica, però, un trattamento di dati personali sanitari o, in ogni caso, sono idonei a rivelare lo stato di salute del lavoratore.

La possibilità di acquisire e utilizzare tale tipologia di dati particolari[294] trova i propri limiti non solo nell'art. 4 SL[295] e nella disciplina *privacy* (come si avrà modo di approfondire successivamente), ma anche

---

290 Il termine "*Internet of things"* (IOT) è stato usato per la prima volta nel 1999 da Kevin Ashton, ricercatore presso il MIT, per descrivere un'architettura erogatrice di servizi collegata ad Internet.
291 In merito Dagnino E., *Le tecnologie per la tutela della salute e sicurezza dei lavoratori tra garanzie e vincoli*, in Lavoro nella Giurisprudenza, n. 6, 2021, pp. 591 ss. Per l'autore, rientrano tra le tecnologie di tipo "esterno" i sistemi di monitoraggio che consentono di verificare lo stato dei dispositivi di protezione (es. giubbotti o scarpe antinfortunistica). Viceversa, nel secondo tipo di tecnologie di monitoraggio rientrano quegli strumenti che servono a tenere traccia della posizione del lavoratore, dei suoi movimenti o dei suoi biosegnali (quali battito cardiaco, temperatura, pressione).
292 In merito ai *wearable device* Ingrao A., *Il braccialetto elettronico tra privacy e sicurezza del lavoro*, in *Diritto delle Relazioni Industriali*, n.3/XXIX, 2019, pp. 895 ss.
293 Fantoni G., Cervelli G., Pira S., Trivelli L., Mocenni C., Zingone R., Pucci T., *Ecosistemi 4.0: imprese, società, capitale umano,* in *Quaderni Fondazione G. Brodolini*, Edizione Fondazione Giacomo Brodolini, Roma, 2017, pp. 56 – 57.
294 Art. 4 GDPR.
295 Per parte della dottrina, il monitoraggio compiuto direttamente sullo stato soggettivo del lavoratore porrebbe tali trattamenti al di fuori dell'ambito applicativo delle discipline in materia di controlli a distanza (ex art. 4 SL) sull'attività dei lavoratori venendo i rilevo, invece, la disciplina inerente al trattamento di dati relativi alla salute dei lavoratori e quella relativa

nella normativa giusalvoristica e di settore e, in particolare, negli articoli 5 e 8 dello Statuto nonché nelle disposizioni dettate dal T.U. in materia di salute e sicurezza sul lavoro (D. Lgs 81/2008).
L'art. 5 SL[296] rubricato "*Accertamenti sanitari*" impone il limite al datore di lavoro di procedere ad accertamenti sanitari in maniera autonoma o avvalendosi di sanitari di sua fiducia, al fine di garantire l'imparzialità e l'obiettività dei controlli[297].
La norma disciplina, dunque, le modalità con cui devono essere eseguite le visite mediche per l'idoneità alla mansione, imponendo l'intermediazione di un medico che non deve essere "di fabbrica"[298], ma caratterizzato dall'indipendenza e terzietà rispetto al datore di lavoro.
Ciò, congiuntamente ai doveri di riservatezza che caratterizzano la professione medica, delinea una preclusione al datore di lavoro di conoscere i dettagli relativi alla salute dei propri lavoratori[299].
Il datore di lavoro è, pertanto, inibito dall'acquisire dati sanitari dei dipendenti che verranno eventualmente comunicati dal medico del lavoro nella sola misura in cui risultino necessari a conoscere lo stato patologico o di infermità dei singoli ai fini dell'assenza o dell'idoneità lavorativa.
Specularmente, l'art. 8 SL[300] sancisce un preciso divieto al datore di lavoro a compiere indagini sulle opinioni dei lavoratori nonché "*su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore*".
La norma dispone un divieto al datore di lavoro - complementare a quello previsto dall'art. 5 SL - di compiere indagini sulle condizioni fisiche del lavoratore e, dunque, di conoscere informazioni relative al suo stato di salute sia nella fase presuntiva che durante lo svolgimento del rapporto di lavoro
Il Legislatore del 1970 aveva, dunque, definito un limite alle pretese conoscitive del datore di lavoro, escludendolo da quelle informazioni che per loro natura (come le opinioni politiche, religiose, sindacali, sanitarie) interessino la sfera personale del lavoratore.
Infine, il TU in materia di salute e sicurezza sul lavoro (D. Lgs. 81/2008), limita la conoscenza del datore in riferimento ai dati sanitari dei lavoratori, secondo una *ratio* analoga a quella prevista dagli artt. 5 e 8 SL.
Il TU del 2008 prevede, infatti, la figura del "medico competente"[301], quale soggetto designato all'acquisizione diretta e all'utilizzo dei dati sanitari dei lavoratori.
Il datore di lavoro è, invece, destinatario delle informazioni che sono ricavabili da tali dati senza entrare, però, in diretto contatto con questi. Il medico competente è, dunque, il soggetto intermediario tra il datore di lavoro e il lavoratore, unico deputato a conoscere le informazioni sanitarie sui lavoratori in maniera dettagliata.

Le norme richiamate stabiliscono, così, un limite al potere datoriale di acquisire informazioni relative la sfera personale del lavoratore, incluse le informazioni relative al suo stato di salute.

---

agli accertamenti dello stato di salute dei dipendenti (ex art. 5 SL e art. 41 D. Lgs. 81/2008). Cfr. Dagnino E., *Le tecnologie per la tutela della salute e sicurezza dei lavoratori tra garanzie e vincoli*, in *Lavoro nella Giurisprudenza*, n. 6, 2021, pp. 591 ss.

296 Art. 5 Stat. lav. "*Accertamenti sanitari*". "1. *Sono vietati accertamenti da parte del datore di lavoro sulla idoneità e sulla infermità per malattia o infortunio del lavoratore dipendente. 2. Il controllo delle assenze per infermità può essere effettuato soltanto attraverso i servizi ispettivi degli istituti previdenziali competenti, i quali sono tenuti a compierlo quando il datore di lavoro lo richieda. 3. Il datore di lavoro ha facoltà di far controllare la idoneità fisica del lavoratore da parte di enti pubblici ed istituti specializzati di diritto pubblico*".

297 Fregni A., Giugni G., *Lo statuto dei Lavoratori*, Giuffrè Editore, Milano, 1971, p. 13; Grandi M. Pera G., *Commentario breve allo Statuto dei lavoratori,* Cedam, Padova, 1985, p. 5.

298 Cfr. Relazione della 10° Commissione del Senato, p. 23.

299 Trojsi A., *Il diritto del lavoratore alla protezione dei dati personali*, Giappichelli Editore, Torino, 2013, pp.175-176.

300 Art. 8 Stat. lav. "*Divieto di indagini sulle opinioni*". "*È fatto divieto al datore di lavoro, ai fini dell'assunzione, come nel corso dello 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*". Per un approfondimento più apio si rinvia al capitolo successivo.

301 Art. 25 TU in materia di salute e sicurezza sul lavoro (D. Lgs. 81/2008).

Il datore di lavoro potrà eseguire accertamenti per tutelare la salute e la sicurezza dei propri preposti, ma senza procedere ad una vigilanza diretta del loro stato di salute.
La tutela prevenzionistica si limita, dunque, ad accertare l'eventuale situazione di rischio al fine di poter intervenire e prevenire stati patologici o di infortunio.
I dati acquisiti da dispositivi digitali dotati di tecnologia *IOT* e adoperati per fini prevenzionistici dovranno, quindi, restituire le sole informazioni strettamente necessarie a tale finalità, monitorando i lavoratori unicamente per il tempo indispensabile a garantire il fine di "salute e sicurezza" per cui sono utilizzati.

***

Svolte tali considerazioni, si procede ad analizzare i rischi inerenti alla salute e sicurezza in riferimento alle prestazioni svolte integralmente in ambienti digitali.

In riferimento alle prestazioni "native digitali" l'individuazione dei rischi correlati al lavoro risulta di nuova definizione e individuazione.
La tutela prevenzionistica è, infatti, una tutela dinamica e necessita di essere modulata rispetto all'evolversi delle modalità di svolgimento della prestazione, tenendo conto dei tempi e dei luoghi di lavoro sempre più fluidi e degli strumenti innovativi impiegati.

Nel caso di prestazioni "native digitali", per analizzare i rischi connessi al lavoro svolto integralmente in ambienti virtuali, non esistendo un riferimento preciso in materia, può essere preso in considerazione quanto dettato in tema di Lavoro Agile[302], in ragione della forte destrutturazione spazio-temporale che tipizza la fattispecie.
Lo svolgimento della prestazione di lavoro in modalità agile non fa venir meno il possesso dei requisiti oggettivi (ovvero quelle di "lavorazioni rischiose") e soggettivi (inerenti alle caratteristiche delle persone assicurate) previsti dal D.P.R. n. 1124/1965 (TU delle disposizioni per l'assicurazione obbligatoria contro gli infortuni sul lavoro e le malattie professionali).
La legge sul Lavoro agile, negli articoli dal 18 al 23, ha così delineato un quadro normativo particolarmente preciso in materia di salute e sicurezza sul lavoro, con particolare riferimento ai rischi connessi allo *stress* lavoro-correlato
L'articolo 19 comma 1 della L. n. 81/2017 prevede, infatti, che nell'accordo individuale sullo *smart working* vengano definite "*le misure tecniche ed organizzative necessarie per assicurare la disconnessione del lavoratore dalle strumentazioni tecnologiche di lavoro*".

[302] Le finalità della disciplina del Lavoro Agile, introdotte dalla Legge n. 81/2017, sono quelle di incrementare la competitività delle imprese agevolando, al contempo, i lavoratori a conciliare i tempi tra lavoro e vita privata (art. 18 comma 1 L. n. 81/2017). In merito anche art. 6 del Protocollo Nazionale sul Lavoro Agile nel settore privato del 7 dicembre 2021 dedicato alla Salute e sicurezza sul lavoro. Il Protocollo stabilisce che ai lavoratori agili trova applicazione la disciplina di cui agli artt. 18, 22 e 23 della L. n. 81/2017, nonché il rispetto degli obblighi di salute e sicurezza previsti dal D. Lgs. n. 81/2008. Inoltre, la prestazione di lavoro in modalità agile deve essere eseguita esclusivamente in ambienti idonei, ai sensi della normativa vigente in tema di salute e sicurezza e di riservatezza dei dati trattati.
Peraltro, il lavoratore agile ha diritto alla tutela contro gli infortuni sul lavoro e le malattie professionali**.** A tal fine, il datore di lavoro garantisce la copertura assicurativa INAIL contro gli infortuni sul lavoro e le malattie professionali, anche derivanti dall'uso dei videoterminali, nonché la tutela contro l'infortunio in itinere, secondo quanto previsto dalla legge.

La norma introduce, così, il "diritto alla disconnessione"[303] rispondendo alla esigenza di assicurare la salute del lavoratore dai rischi di *overworking* e, in particolare, dai rischi di iperconnessione e di dipendenza tecnologica.
L'istituto, che trova il suo modello nell'ordinamento francese[304], consiste nel diritto del lavoratore a rendersi "irrintracciabili" dal datore di lavoro senza subire conseguenze negative.
Il diritto alla disconnessione si articola in una duplice definizione: il diritto di disconnessione dal lavoro (volto a tutelare salute e tempo libero) e il diritto alla disconnessione sul lavoro (funzionale a prevenire disturbi dovuti ad un'eccessiva sollecitazione da parte di dispositivi informatici).
Il "diritto alla disconnessione" viene menzionato anche dal recente Protocollo Nazionale sul Lavoro Agile nel settore privato (sottoscritto il 7 dicembre 2021) che, all'art. 3, si propone di regolare la disconnessione dei lavoratori agili. In particolare, il Protocollo sottolinea come l'attività lavorativa svolta in modalità agile si caratterizzi per l'assenza di un preciso orario di lavoro e per l'autonomia nello svolgimento della prestazione. Conseguentemente, invita ad individuare la fascia di disconnessione nella quale il lavoratore non debba erogare la prestazione lavorativa, prevedendo l'adozione di misure tecniche e/o organizzative per garantirne il rispetto.

La normativa sullo *smart working* introduce, così, uno dei principali rischi rimessi al lavoro digitale, ovvero il verificarsi di problemi psicosociali quali sono lo *stress* lavoro-correlato e il disequilibrio tra l'attività lavorativa e la vita privata.
Il rischio da iperconnessione o il manifestarsi di *stress* lavoro-collegato, anche in reazione ad una socialità alterata rispetto a quella del lavoro in presenza, appare, dunque, riscontrabile in tutte le prestazioni che vengono eseguite principalmente, se non esclusivamente, in un ambiente digitale.

In merito, anche l'Agenzia Europea per la Salute e Sicurezza sul Lavoro nel documento redatto sulla previsione dei rischi nuovi ed emergenti per la salute e sicurezza del lavoro associati alla digitalizzazione entro il 2025 indica che le nuove tecnologie "*possono consentire alle persone di lavorare sempre e ovunque. Ciò potrebbe portare a una confusione tra il lavoro e la vita privata delle persone in termini sia di attività che di sicurezza e salute, compreso un impatto negativo sulla salute mentale e sul benessere. La capacità delle nuove tecnologie di abilitare al lavoro in qualsiasi momento potrebbe portare a un'esigenza reale o percepita di essere disponibili tutto il giorno, tutti i giorni (24 ore su 24, 7 giorni su 7). Ad esempio, le persone potrebbero dover lavorare con colleghi in un fuso orario diverso. Ci sono anche preoccupazioni che le persone possano soffrire di dipendenza dall'uso di dispositivi mobili e dispositivi indossabili simili, che l'utente soffra di grave ansia se separato dal dispositivo o se smette di funzionare, nota anche come "dipendenza digitale" (…). Questo potrebbe aumentare man mano che tali dispositivi diventano più diffusi, evoluti e necessari per il lavoro o la vita in generale. La disponibilità 24 ore su 24, 7 giorni su 7, potrebbe avere impatti sulla salute e sicurezza sul lavoro simili al lavoro a turni, come il cancro, in particolare quando le persone lavorano di notte (IARC, 2007), il diabete e le malattie cardiovascolari (Research EU Results Magazine, 2017). Alcuni lavoratori potrebbero considerare di essere visti 24 ore su 24, 7 giorni su 7, un segno di successo, ma comunque soffrire di cattiva salute, stress e/o burnout di conseguenza"*[305].

303 Al diritto alla "disconnessione" parte della dottrina individua uno speculare "dovere di disconnessione" che spetta al datore di lavoro disciplinare nel quadro della nuova organizzazione del lavoro per "fasi, cicli e obiettivi" che caratterizza il lavoro agile. In merito Dagnino E., *Il diritto alla disconnessione nella legge n. 81/2017 e nell'esperienza comparata*, in *Diritto della Relazioni Industriali (DRI),* n. 4, 2017, pp. 1024 ss.
304 Art. 55 contenuto nel titolo *Adaptation du droit du travail à l'ère numérique* della *Loi Travail*. In merito Morel L., *Le droit à la déconnexion en droit français. La question de l'effectivité du droit au repos à l'ère du numérique, Labour & Law Issues* (*LLI*), vol. 3, n. 2, 2018, pp. 5 ss.
305Agenzia Europea per la Salute e Sicurezza sul Lavoro, *Foresight on new and emerging occupational safety and health risks associated with digitalisation by 2025,* pp. 10-11, disponibile *online.*

L'individuazione di tali rischi associa una richiesta del Legislatore al datore di lavoro di svolgere una "vigilanza", al fine di evitare il verificarsi dei fenomeni dannosi.

Altri rischi connessi alle prestazioni digitali riguardano l'uso continuativo di videoterminali per l'esecuzione della prestazione (Titolo VII del TU in materia di salute e sicurezza sul lavoro - esposizione ai videoterminali), oltre agli obblighi specifici connessi all'allestimento della postazione di lavoro (rischi ergonomici inerenti alla postura, illuminazione, temperatura dei locali).
In relazione all'uso degli strumenti di lavoro, infatti, l'art. 18 comma 2 della L. n. 81/2017 prevede che "*il datore di lavoro è responsabile della sicurezza e del buon funzionamento degli strumenti tecnologici assegnati al lavoratore per lo svolgimento dell'attività lavorativa*".

Ora, mentre per quanto riguarda le attività di prevenzione per i rischi connessi all'uso di videoterminali o alla postazione di lavoro, il controllo a fini prevenzionistici interesserà lo strumento o il posto dove viene eseguita la prestazione e prevedrà un (necessario) obbligo di cooperazione[306] del lavoratore (ove la prestazione sia resa fuori dai locali aziendali), per quanto riguarda il rischio da iperconnessione o da *stress*-lavoro correlato, il datore di lavoro può eseguire una vigilanza attiva attraverso gli strumenti con cui la prestazione viene resa.
In particolare, l'utilizzo di *Digital Workplace*, consentendo seguire ogni "*click*" o traccia digitale dei lavoratori, potrebbe fungere da supporto per verificare che le attività non siano svolte in modalità *overworking*.
Per poter compiere tale verifica è necessario, però, procedere a un'acquisizione e a una successiva elaborazione dei dati.
Solo tramite la loro correlazioni e interpretazione è possibile, infatti, accertare se il lavoratore digitale ha eseguito prestazioni per un periodo prolungato, rimanendo connesso alla *Digital Workplace* oltre i tempi definiti.
Accedere ai dati provenienti da tali strumenti e impiegarli per tutelare la salute e la sicurezza del lavoratore è cosa ben diversa, però, dallo scaricare le registrazioni di una telecamera collocata in un ambiente fisico di lavoro.
Le immagini acquisite dalla telecamera saranno, infatti, "autoevidenti" e capaci di rappresentare in maniera immediata l'eventuale situazione di rischio.
Diversamente, i dati acquisiti da ambienti digitali dovranno essere elaborati al fine di rendere comprensibile quanto registrato.
Elaborazione che può interessare anche (e soprattutto) dati non organizzati come gli *exhaust data* che in quanto "scarti" di operazioni principali compiute dal lavoratore potrebbero restituire una descrizione delle interazioni compiute.
Il monitoraggio a fini prevenzionistici delle prestazioni all'interno di una *Digital Workplace* può, quindi, restituire un'indicazione del livello di *stress* lavoro-correlato sofferto dal lavoratore.
La vigilanza dovrà, però, passare per una fase di elaborazione di dati, la maggior parte dei quali non strutturati, come possono essere documenti prodotti dal lavoratore, numero di interazioni compiute (o non compiute) o tempistica nell'esecuzione di richieste.

[306] In base all'art. 20 del D. Lgs. n. 81/2008 il lavoratore deve dare il proprio contributo all'attuazione delle misure di prevenzione predisposte dal datore di lavoro per fronteggiare i rischi connessi all'esecuzione della prestazione all'esterno dei locali aziendali.

Nel caso delle prestazioni "native digitali", il controllo per determinati rischi e, in particolare, per il rischio di iperconnessione e di *stress* lavoro-correlato comporta necessariamente due fasi: l'acquisizione dei dati e la loro elaborazione per la comprensione.
La legittimazione di tali operazioni (fondata sulle esigenze di cui all'art. 4 comma 1 SL) può determinare, però, la possibilità di acquisire informazioni eccedenti quelle strettamente necessarie per sorvegliare tali rischi.
L'elaborazione di dati non strutturati rende potenzialmente accessibile al datore di lavoro elementi da cui potrebbero essere ricavate informazioni ultronee e atte a rivelare aspetti personali dei lavoratori.

La finalità della tutela della salute e sicurezza in un contesto di prestazioni "native digitali" sembrerebbe poter "aprire la strada" ad una serie di analisi sofisticate compiute su dati apparentemente privi di importanza, ma inidonei a fornire un tracciamento estremamente accurato dell'attività dei lavoratori.
Potrebbe, inoltre, consentire l'esecuzione di elaborazioni su dati acquisiti da fonti normalmente interdette (come il numero di interazioni compiute nello spazio virtuale), la cui analisi potrebbe rilevare molto di più dello stato psico-fisico del lavoratore.
Infine, l'utilizzo mediante interpretazione di tali dati potrebbe consentire al datore di lavoro di compiere una "sorveglianza sanitaria diretta" (vietata) anche ai fini di valutare l'idoneità lavorativa dei lavoratori da un punto di vista delle propensioni e capacità di affrontare condizioni stressanti.
Il processo di elaborazione di un flusso di dati non "autoevidenti" rende così incerto il momento in cui le tutele previste dall'ordinamento (in particolare dagli artt. 5 e 8 SL e dal D. Lgs. 81/2008) si possono considerare pienamente operanti.
Infatti, la mera acquisizione di dati apparentemente "neutri" non integra la condotta vietata che verrebbe a rivelarsi solo con la successiva elaborazione dei dati.

L'elaborazione di dati "non autoevidenti" per fini prevenzionistici potrebbe, quindi, far collimare gli obblighi imposti dall'ordinamento a condotte vietate dallo stesso.

L'ulteriore rischio connesso all'elaborazione dei dati è quello di riuscire a tracciare, mediante le tecniche di *Data Analysis,* una profilazione dei lavoratori in riferimento alle caratteristiche rilevate inerenti allo stato di salute.
Al pari di quanto realizzato dall'INPS con il *software* Savio che, avvalendosi di tale applicativo, dall'8 febbraio 2011 al marzo 2018 ha analizzato i dati personali di 12,6 milioni di lavoratori pubblici assenti per malattia.
La finalità dell'Istituto era quella di organizzare le visite fiscali in maniera cadenzata, verificando e individuando preventivamente le possibili assenze ingiustificate e i comportamenti fraudolenti[307].
Per fare ciò, il *software* SAVIO attribuiva alle certificazioni di malattia un punteggio di maggiore o minore affidabilità su base statistica in relazione al giudizio prognostico di idoneità alla ripresa del lavoro o di assenza ingiustificata.
Il sistema procedeva senza prendere in considerazione la diagnosi (ossia la "malattia" da cui è affetto il lavoratore), ma analizzando la frequenza e la durata dei singoli episodi di malattia insieme ad altre variabili

[307] Cfr. Messori G., *Utilizzo di modelli statico-predittivi e data mining: il caso INPS e alcune guidelines operative*, in *Cyberlaws,* 24 settembre 2018, disponibile su www.cyberlaws.it.

quali il numero delle precedenti idoneità alle visite mediche di controllo, la qualifica del lavoratore, il tipo di rapporto in essere, la retribuzione, e la dimensione aziendale[308].
In ragione delle potenzialità di analisi riconosciute a SAVIO, però, il Garante per la Protezione dei Dati Personali ha sanzionato l'Istituto per violazione della normativa *privacy*[309], proprio perché l'applicativo acquisiva nuove informazioni, qualificate come particolari, a seguito dell'elaborazione di dati apparentemente "neutri".

Dalla disamina appare come la soglia di criticità del controllo si ritrovi non più nel momento di acquisizione dei dati, ma in quello in cui questi vengono analizzati anche se per fini meritevoli come quello di tutelare la salute e sicurezza dei lavoratori.
Il rischio intrinseco è quello di travalicare la finalità e di compiere un controllo sproporzionato e diretto su aspetti altamente sensibili, come le condizioni psico-fisiche di una persona.

2.5. Esigenze di tutela del patrimonio aziendale: la sicurezza informatica

La tutela del patrimonio aziendale è l'ultima delle esigenze di controllo "preterintenzionale" introdotta dal Legislatore con la riforma del 2015.
Grazie a tale previsione, i datori di lavoro sono autorizzati a procedere a controlli per la tutela dei propri beni, sempre nel rispetto delle prescrizioni dell'art. 4 SL, salvo non si configuri la fattispecie di "controllo difensivo in senso stretto"[310].
Orbene le imprese odierne, dotate di strumenti digitali, dovranno tutelare anche le tecnologie utilizzate, inclusi i dispositivi informatici, gli applicativi e i sistemi di abilitazione al *web*.
La necessità di tutelare tali beni risponde non solo a logiche di interesse aziendale, ma anche a un preciso dovere che grava i capo al datore di lavoro che riveste il contestuale ruolo di Titolare del trattamento, ai sensi dell'art. 4 par. 1 n. 7 del GDPR[311].
Il Titolare del trattamento è, infatti, tenuto a mettere "*in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento effettuato è conforme*"[312] al GDPR.
Il datore di lavoro dovrà, pertanto, accertare che i sistemi informatici che impiega per lo svolgimento della gestione dei lavoratori e per l'esecuzione delle prestazioni digitali siano "sicuri" da un punto di vista tecnico (oltre che organizzativo) nel trattamento dei dati acquisiti.
Il GDPR prevede, infatti, che i datori di lavoro siano responsabili[313] dei trattamenti posti in essere, garantendo che i dati siano protetti, salvaguardandone la perdita, la distruzione o il danneggiamento.
Il Regolamento a riguardo suggerisce una serie di misure di sicurezza che possono essere utilizzate per assicurarne la protezione[314].

---

308 Cfr. Audizione Presidente Inps, prof. Tito Boeri, del 6 settembre 2018. Visite mediche di controllo d'ufficio – metodologie di *data mining* – procedimento sanzionatorio del Garante per la protezione dei dati personali avanti alla XI Commissione permanente lavoro pubblico e privato, previdenza sociale del Senato.
309 GPDP, Ordinanza/ingiunzione n. 92 del 29 novembre 2018.
310 In merito si rinvia al capitolo 2 punto 1.4.2
311 A norma dell'art. 4 SL il Titolare del trattamento è "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri*".
312 Art. 24 par. 1 GDPR.
313 In base al "principio di *accountability*" introdotto dal GDPR.
314 Tra cui figurano la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento (art. 32 par. 1 lett. b GDPR), la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico (art. 32 par. 1 lett. c GDPR), nonché di adottare una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche al fine di garantire la sicurezza del trattamento (art. 32 par. 1 lett. d GDPR).

Con la digitalizzazione e l'adozione di tecnologie ICT la possibilità di connettersi alla rete diviene uno dei principali vantaggi per le imprese, ormai comunemente diffusa in tutte le organizzazioni.
È, per esempio, consuetudinario l'impiego di posta elettronica e l'utilizzo per fini lavorativi di dispositivi connessi alla rete.
Grazie alla connessione *Internet,* il lavoro può essere remotizzato, abilitando l'accesso a piattaforme digitali o luoghi di lavoro virtuali (quali le *Digital Workplace*).
La medesima tecnologia di connessione alla rete è integrata anche nei sistemi di gestione (quali i *HRIS* e *CRM*) al fine di favorire la centralizzazione delle informazioni e la disponibilità delle stesse.

In tutti questi casi, il datore di lavoro è responsabile dell'utilizzo degli strumenti tecnologici e della sicurezza dei dati trattati.
Si deve, infatti, precisare che l'utilizzo di strumenti informatici connessi al *web* è un'attività che comporta il trattamento di dati personali[315] ove l'utente (ovvero il lavoratore) sia identificabile.
Il concetto di dato personale fa riferimento a informazioni che possono essere anche indirettamente ricondotte a un individuo. In particolare, l'art. 4 del GDPR prevede che un dato personale sia "*qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a (…) un identificativo online (…)*".
Il concetto di identificativo *online* è stato definito in modo ampio dalla Corte di Giustizia dell'Unione Europea[316] la quale ha chiarito che sono dati personali sia l'indirizzo *IP* statico sia l'indirizzo *IP* dinamico, intendendo per *IP* statico il numero univoco di identificazione assegnato sempre allo stesso dispositivo di una rete (come un PC collegato a *Internet*) e per *IP* dinamico il numero univoco che viene assegnato e cambiato automaticamente ad ogni nuova connessione. Mediante entrambi gli *IP* è, infatti, possibile risalire all'identità dell'utente che li utilizza.
Concordemente, il Garante per la Protezione dei Dati Personali (GPDP)[317] ha più volte indicato il *MAC address* come un dato personale, considerando identificabile l'indirizzo associato a ciascuna scheda di rete integrata in ogni *PC* o dispositivo mobile. Si tratta, infatti, di un identificativo univoco che viene imposto dal proprietario di *hardware* della singola scheda.
Di conseguenza, devono considerarsi dati personali la data e l'ora della connessione e della disconnessione del servizio di accesso al *web* da parte di un utente identificabile, i dati di traffico che rivelano la durata delle connessioni, la loro collocazione temporale, il contenuto della navigazione e anche il luogo fisico ove vengono effettuate (qualora si tratti di dispositivi mobili)[318].

Pertanto, venendo trattati dati personali dei lavoratori, il datore di lavoro è tenuto ad adottare idonee misure tecniche che tutelino i propri sistemi da possibili minacce che provengano dal *web.*
I sistemi posti a controllo della sicurezza informatica per la navigazione su *Internet* possono, però, fornire anch'essi informazioni sulle attività svolte dai lavoratori in rete e sulle (eventuali) violazioni commesse.
Per tale ragione è necessario analizzare brevemente alcuni dei sistemi adottati per connettersi alla rete *Internet* e per tutelare l'integrità dei beni aziendali da eventuali rischi associati.

315 Come definito dall'art. 4 n. 2 GDPR.
316 Corte di Giustizia Europea, sentenza nella causa C-582/14 Patrick Breyer/Bundesrepublik Deutschland, del 19 ottobre 2016.
317 GPDP provvedimento del 13 luglio 2016, n. 303, doc. web. n. 5408460.
318 GPDP provvedimento del 13 maggio 2021, n. 190, doc. web n. 9669974. In merito Ingrao A., *Il potere di controllo a distanza sull'ozio telematico e il limite del diritto alla privacy del lavoratore*, in Rivista Italiana di Diritto del Lavoro, vol. 3, 2019, pp. 416 ss.

Il *browser Internet*

Ogni volta che un lavoratore si connette a *Internet* accede mediante un programma di *browser*.

L'utilizzo dei *browser* consente alle imprese di poter conoscere, attraverso i propri *file* storici, tutte le connessioni e le pagine scaricate dai dipendenti.

Ogni sito *web* è, infatti, dotato di un proprio URL univoco (*Uniform Resource Locator*), preceduto dalle lettere "http://" (*Specific Internet Protocol*).

Tutti i *browser Internet* hanno una funzione chiamata "Cronologia" che tiene traccia di tutti i siti (*URL*) visitati dall'utente durante la navigazione sul *web*.

Attraverso la Cronologia si possono, così, ottenere informazioni sule pagine (URL) visitate, il numero di visite a ciascuna delle pagine, la data e l'ora degli accessi, la durata e molto altro.

Appare chiaro che l'accesso a tali informazioni da parte del datore di lavoro, anche se compiuto per garantire la sicurezza dei dispositivi aziendali, permetta di acquisire un gran numero di dati sulle attività realizzate dai lavoratori.

Il *firewall*

Un *firewall* è un sistema utilizzato per proteggere la rete aziendale da possibili attacchi esterni che potrebbero compromettere la sicurezza dell'impresa.

Lo scopo del *firewall* è quella di fungere da ponte tra la rete locale (da proteggere) e la rete *Internet* a cui ci si vuole connettere.

In questa maniera la circolazione delle informazioni tra le due reti risulta controllata.

Un *firewall* stabilisce, quindi, una serie di filtri e verifica gli indirizzi *Internet* a cui è possibile accedere mediante la rete aziendale.

Il *firewall* è anche in grado di restituire una serie di *report* sui tentativi di accesso da o verso siti interdetti alla navigazione.

Il monitoraggio e la stesura di *report* da parte dei *firewall* sono, quindi, operazioni in grado di restituire informazioni sui lavoratori che accedono a *Internet* attraverso la rete aziendale.

Il *Cookie*

Un altro tipo di sistema che può essere utilizzato per monitorare l'utilizzo di *Internet* da parte dei dipendenti sono i *Cookies*.

Il *Cookie* è un piccolo *file* di testo che viene memorizzato sul disco rigido del PC, utilizzato dal lavoratore, salvo che questo non venga eliminato.

I *Cookies* hanno due funzioni: la prima è mantenere lo stato di applicazione. In questo caso, il *Cookie* permette, per esempio, di tornare su un sito mantenendo le impostazioni adottate o iniziare dalla pagina da cui si era interrotta la navigazione.

La seconda è eseguire un tracciamento sul *web*, permettendo di conoscere le abitudini dell'utente durante la navigazione in rete, memorizzando i siti visitati dall'utente e le azioni intraprese.

Anche in quest'ultima ipotesi, può avvenire un monitoraggio delle attività svolte dal lavoratore.

***

Il monitoraggio tramite strumenti digitali e dispositivi per tutelare l'integrità dei beni aziendali è una (inevitabile) fonte di acquisizione di ingenti volumi di dati.

Dati che, permettendo di identificare il soggetto, possono monitorare l'attività del lavoratore e che potrebbero essere impiegati per tutelare i beni aziendali anche al di fuori dell'ambito (e delle tutele) dell'art. 4 SL.

Si deve, infatti, tenere in considerazione che la giurisprudenza sui "controlli difensivi in senso stretto" ammette la conferma *ex post* della legittimità del controllo occulto compiuto, a patto che sussista il fondato sospetto della condotta illecita del lavoratore[319].
La convalida di tale ricostruzione si trova anche nella recente pronuncia della Suprema Corte del 22 settembre 2021 n. 25732. Nel caso di specie, la Corte ha ritenuto legittimo un licenziamento intimato a seguito di accertamenti compiuti sul *computer* di una dipendente in ragione dei danni causati da un *malware* alla rete informatica aziendale.
L'ispezione compiuta dall'azienda appurava che il *virus* era stato introdotto nella rete attraverso un *file* scaricato dalla lavoratrice che aveva visitato pagine *web* estranee all'attività lavorativa.
Per tale motivo, la dipendente veniva sanzionata, avendo utilizzato strumenti informatici per fini extra lavorativi e causando, con tale condotta, danni al patrimonio aziendale.
La Corte di Cassazione ha rigettato il ricorso della dipendente, qualificato il controllo condotto dal datore di lavoro come "controllo difensivo in senso stretto", estraneo ai limiti imposti dall'art. 4 SL, poiché diretto ad accertare gravi illeciti compiuti dalla singola lavoratrice[320].
Il caso richiamato evidenzia come il monitoraggio eseguito in ragione di un "controllo difensivo in senso stretto" esuli dalle tutele proprie della norma statutaria.

I controlli per tutelare la rete aziendale possono, inoltre, essere eseguiti anche su singoli applicativi ove si accerti un'eventuale compromissione di sistema.
Anzi, taluni servizi o *software* impiegati per garantire la sicurezza vengono ricondotti dal GPDP alla nozione di strumento di lavoro.
Sono, infatti, considerati "strumenti di lavoro" quegli applicativi *"che ne consentono il fisiologico e sicuro funzionamento al fine di garantire un elevato livello di sicurezza della rete aziendale messa a disposizione del lavoratore (ad esempio: sistemi di logging per il corretto esercizio del servizio di posta elettronica, con conservazione dei soli dati esteriori, contenuti nella cosiddetta envelope del messaggio, per una breve durata non superiore comunque ai sette giorni; sistemi di filtraggio antivirus che rilevano anomalie di sicurezza nelle postazioni di lavoro o sui server per l'erogazione dei servizi di rete; sistemi di inibizione automatica della consultazione di contenuti in rete inconferenti rispetto alle competenze istituzionali, senza registrazione dei tentativi di accesso)*"[321].
Il controllo per la realizzazione della sicurezza informatica sarà, dunque, legittimo e riconducibile alla nozione di strumento di lavoro (*ex* art. 4 comma 2 SL) ove sia funzione all'attuazione della tutela del patrimonio aziendale ove dotato di limitazioni nelle modalità di monitoraggio, anche temporali.

***

Da quanto riportato traspare come la finalità di tutela del patrimonio aziendale, qualora interessi dispositivi informatici impiegati dall'azienda, implementi le fonti di acquisizione dei dati afferenti ai lavoratori.

---

319 Cfr. Maresca A., *Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 dello Statuto dei lavoratori*, in *Rivista Italiana di Diritto del Lavoro (RIDL)*, vol. I, n. 4, 2016, pp. 513 ss.
320 Per la Corte di Cass. del 22 settembre 2021 n. 25732, dunque, il datore di lavoro ove sospetti che un dipendente stia commettendo un illecito può quindi effettuare controlli a distanza utilizzando strumenti tecnologici senza seguire le rigide procedure previste dallo Statuto dei lavoratori. Tale controllo deve però essere attuato solo dopo che il datore di lavoro abbia avuto il fondato sospetto che sia stato compiuto un illecito da parte di uno o più lavoratori. Questo tipo di controllo può inoltre estendersi solo alla raccolta delle informazioni acquisite da quel momento in poi e non può riguardare invece informazioni e dati acquisiti senza il rispetto dell'art. 4 dello Statuto dei lavoratori prima di quel momento, al fine di non estendere a dismisura l'area del controllo difensivo.
321 Garante per la Protezione dei Dati Personali (GPDP) prov. n. 303 del 13 luglio 2016.

Tali strumenti sono, inoltre, capaci di restituire un monitoraggio accurato di ogni attività compiuta dagli utenti durante il loro utilizzo e, in gran parte dei dati acquisiti, sono qualificabili come "non autoevidenti". Rientrano, infatti, nella categoria degli *exhaust data*[322] il percorso di *clic* compiuto da un utente su una pagina *web*, oppure i dati di traffico di *e-mail* e calendario, che forniscono informazioni sul comportamento dei soggetti tra loro in relazione.
Tutte informazioni che possono essere monitorate per tutelare la sicurezza del patrimonio aziendale.

L'acquisizione di dati per salvaguardare il patrimonio informatico dell'impresa abilita così a potenziali elaborazioni, anche di informazioni non comprensibili, ammettendo (per certi versi) un controllo ancora più pervasivo in relazione a quello compiuto per altre finalità di cui all'art. 4 SL.
Si deve, infatti, ricordare che la giurisprudenza ammette la possibilità che vengano eseguiti controlli occulti per esigenze difensive dell'impresa.
L'analisi dei dati potrebbe, perciò, consentire non solo un controllo diretto o sproporzionato, ma anche di far sorgere quel "fondato sospetto" di un illecito (elemento giustificatore di un "controllo difensivo in senso stretto") anche quando l'infrazione non si sia ancora verificata.
Sarebbe l'elaborazione, infatti, a individuare i comportamenti "sospetti" che, per logica computazionale, appaiono statisticamente rilevanti ai fini di un'eventuale violazione.
Una situazione alla "*Minority report*"[323] che legittimerebbe un controllo sul lavoratore in assenza delle tutele previste dalla normativa statutaria.

Si deve, inoltre, considerare che alcuni *software* o servizi impiegati per garantire la sicurezza esulano dalla stessa nozione di "strumento di controllo" quando consentono il fisiologico e sicuro funzionamento al fine di garantire un elevato livello di sicurezza della rete aziendale messa a disposizione del lavoratore.
In tale circostanza, la ponderazione sulla legittimità del controllo permarrebbe, ma verrebbe meno la necessaria autorizzazione preventiva.

La tutela del patrimonio informatico aziendale si presenta, quindi, non solo come un'ulteriore fonte di dati acquisibili sui lavoratori, ma appare anche scevra da alcune delle tutele poste a garanzie degli stessi.

2.6. Alcune considerazioni conclusive

Le tecnologie impiegate nell'ambito della gestione dei lavoratori e le capacità analitiche delle stesse pongono nuove criticità in relazione all'esercizio del potere di controllo datoriale dovute sia alla maggiore quantità dei dati raccolti nei contesti lavorativi digitali sia (e soprattutto) alle modalità di elaborazione degli stessi.
L'analisi dei dati comporta, infatti, la creazione di nuove informazioni inerenti ai dipendenti e alla loro attività lavorativa, direttamente accessibili al datore di lavoro.
La *ratio* posta a fondamento della norma risulta valida e attuale, ma la tutela che la stessa si prefigge di garantire sembra attenuarsi.
Il principio posto alla base dell'art. 4 SL riguarda "*la dimensione personalistica, l'intenzione di tutelare la privatezza del lavoratore di fronte all'occhio scrutatore e onnipresente di un Grande Fratello aziendale*"[324].

---

322 In merito si rinvia al capitolo 1 punto 3.
323 Racconto fantascientifico di Philip K. Dick ove la polizia, grazie a un sistema chiamato "*Precrimine",* riesce a impedire gli omicidi prima che essi avvengano e ad arrestare i potenziali "colpevoli".
324 D'Antona M., *L'art. 4 dello Statuto dei Lavoratori ed elaborati elettronici*, in De Luca Tamajo R., Imperiali D'Afflitto R., Pisani C., Romei R. (a cura di), *Nuove tecnologie e tutela della riservatezza del lavoratore*, Giuffrè Editore, Milano, 1988, pp. 204-205.

Il controllo a distanza ammesso è, dunque, quello esercitato dall'uomo sull'uomo e non dalla macchina sull'uomo.

In un contesto "analogico", ove il prestatore può essere osservato mediante dispositivi audiovisivi o di registrazione della parola, il potere di controllo del datore di lavoro coincide con il momento di acquisizione del dato.
L'utilizzo di strumenti che registrano un'attività lavorativa compiuta "in presenza" restituiscono, infatti, un'informazione immediatamente comprensibile, ovvero "autoevidente", prontamente spendibile dal datore di lavoro.
Il momento in cui viene esercitato il controllo coincide, dunque, con quello di recepimento del dato, non essendo necessaria alcuna elaborazione intermedia.

Quando, però, si passa ad osservare una prestazione compiuta interamente in un "ambiente di lavoro digitale", il binomio "acquisizione del dato - esercizio del potere di controllo" sembra affievolirsi.
La prestazione "nativa digitale", ovvero quella che nasce in un contesto informatico, non sempre è immediatamente comprensibile.
I dati estrapolati da contesti digitali possono risultare "non strutturati" oppure "di scarico" (come gli *exhaust data)* e dunque dimostrarsi "non autoevidenti".
Acquisire dati "non significativi" sposterebbe, così, il momento in cui viene esercitato il potere di controllo nella fase successiva di interpretazione che si realizza mediante il supporto (necessario) di *software* o sistemi di A.I.
Tant'è vero che sembrerebbe potersi parlare di un momento di "monitoraggio" (ovvero di acquisizione dei dati) distinto rispetto al momento di "controllo" dei lavoratori (in cui i tati vengono interpretati).
Il potere datoriale viene così rappresentato da un nuovo e composito "potere informatico"[325] o "computazionale"[326] abilitato non solo al controllo, ma ad elaborare i dati dei lavoratori in maniera anche completamene automatizzata grazie al supporto di sofisticate tecnologie informatiche.
Il potere di controllo "computazionale" si avvarrebbe, quindi, di strumenti capaci di processare i dati e di ottenere informazioni nuove e ulteriori rispetto a quelle acquisite, in alcuni casi non rintracciabili in altro modo.
Informazioni che possono esorbitare l'ambito professione e porre in essere "profilature" dei singoli lavoratori anche in riferimento alla sfera personale e privata.

Supportati dalle capacità di produrre informazioni proprie dei sistemi di *Algorithmic Management,* i poteri datoriali acquistano, in tal modo, una rinnovata forza e pervasività[327].
Il controllo tecnologico verrebbe a compiere una sorveglianza "disumana" (ovvero compiuta della macchina sull'uomo) non più a causa del mezzo utilizzato per acquisire le informazioni, ma in ragione del processo di elaborazione.
Secondo tale ricostruzione, il controllo evolverebbe in una forma più "sofisticata", non limitandosi a un'osservazione "autoevidente", come può essere lo *screenshot* di un videoterminale a cui è impegnato il lavoratore.

---

325 Cfr. Trojsi A., *Potere informatico del datore di lavoro e controllo sui lavoratori, cinquant'anni dopo*, in dirittifondamentali.it, n. 2, 2020, p.1414; Trojsi A., *Controllo a distanza (su impianti e strumenti di lavoro) e protezione dei dati del lavoratore*, in *Variazioni su Temi di Diritto del Lavoro*, n. 4, 2016, p. 667.
326 Cfr. Durante M., *Potere computazionale. L'impatto delle ICT*, in *Diritto società e sapere,* Meltemi, 2019.
327 In merito alcuni interpreti ipotizzano la sussistenza di un "potere di controllo direttivo". Cfr. Tebano L., *Lavoro, potere direttivo e trasformazioni organizzative*, Editoriale Scientifica, 2020, p. 239.

L'utilizzo di tecniche di *Data Analysis* comporta, quindi, rischi connessi alle caratteristiche dei processi che li generano, orientati a calcolare statisticamente le correlazioni tra dati.
L'elaborazione dei dati può, infatti, far emergere "*inferenze non prevedibili, fenomeni non ricercati (…) rispetto ai quali (in quanto ignoti ex ante) non sarebbe comunque possibile un campionamento preventivo*"[328], venendosi a creare una sorta di "*subconscio digitale*"[329].
La gestione del lavoro ha, dunque, assunto le caratteristiche della datificazione, accedendo alle potenzialità introdotte dalla stessa e comprendendo il valore rimesso all'analisi dei dati e alle loro correlazioni.

Al termine della disamina che si è prefissa di fungere come una sorta di "*crash test*" della normativa giuslavoristica, si può comprendere come l'esercizio del controllo negli ambienti digitali avviene, di fatto, non più quando i dati vengono acquisiti (perno della tutela statutaria), bensì quando questi sono compresi ed elaborati.
La normativa giuslavoristica si ferma sulla "soglia" di quella che è la vera rivoluzione del potere datoriale: trarre informazioni in modo indiretto, ma capaci di eseguire un preciso controllo del lavoratore.
Controllo che, mediante l'utilizzo dei dati, può mutare la propria natura da preterintenzionale a diretto senza che, a memoria di quanto esposto dal comma 1 dell'art. 4 SL., la norma risulti violata.

La stessa norma giuslavoristica sembra, inoltre, non riuscire a limitare anche la raccolta diffusa di dati. Quando, infatti, le prerogative datoriali rientrano nelle esigenze elencate dalla legge, nessun limite viene apposto alla quantità di dati che possono essere acquisiti ove afferenti alla finalità dichiarata.
Volume che può essere, potenzialmente, ingente.
E tanto maggiori saranno i dati raccolti, tanto aumenterà la possibilità di elaborarli per trarne ulteriori informazioni.

L'esercizio del potere di controllo diviene, pertanto, il "canale preferenziale" di accesso alle informazioni posto che il monitoraggio attraverso strumenti digitali è una fonte inesauribile di dati[330].
Si tratta di un processo "evolutivo" di cui il diritto deve avere consapevolezza, senza rimanere legato a categorie superate in quanto "analogiche", in taluni casi inapplicabili al nuovo lavoro "nativo digitale" profondamente distinto nelle esigenze e nei presupposti fattuali di tutela.
Il controllo a distanza di un lavoro analogico non ha mai dovuto interrogarsi sul significato dell'informazione registrata.
"L'universo parallelo" della prestazione "nativa digitale" pone quale primario interesse quello di comprendere cosa significhino i flussi di dati acquisiti.

Ciò posto, ci si domanda se le tutele previste dalla normativa *privacy*, strettamente connesse alla norma giuslavoristiva a seguito della riforma del 2015, siano in grado di ovviare a tali problematiche, conformando la disciplina alle nuove esigenze di salvaguardia del lavoro digitale.

---

328 Mantelero A., *Big Data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, in *Il Diritto dell'Informazione e dell'Informatica,* n. 1, 2012, p. 138.
329 Il termine "subconscio digitale" fa riferimento alla circostanza che "*l'interessato potrebbe perfino non sospettare l'esistenza di altre informazioni 'neonate' su di sé*". In merito Mazzotti M., *Per una sociologia degli algoritmi*, in *Rassegna Italiana di Sociologia*, n. 3-4, 2015, p. 465.
330 In merito Donini A., *Tecniche avanzate di analisi dei dati e protezione dei lavoratori*, in *Diritto delle Relazioni Industriali (DRI*), n. 1, 2018, p. 230.

A tale quesito si cercherà di dare una risposta nell'ultimo capito dopo aver compiuto una disamina sulle criticità connesse all'esercizio del potere computazionale (capitolo 3) e sulla possibilità di acquisire nuove informazioni sui prestatori, anche mediante l'analisi svolta da sistemi integralmente automatizzati (capitolo 4).

Capitolo 3
Ulteriori criticità connesse all'elaborazione dei dati

1. Il controllo inferenziale

Dalla ricognizione compiuta emerge come, nei rapporti di lavoro, la condivisione d'informazioni sia un elemento costante.
Mediante i differenti applicativi informatici vengono, infatti, trattati dati del lavoratore sia di natura personale (come nome e cognome, indirizzo, qualifiche lavorative) che, talvolta, particolare (come lo stato psicofisico).
Lo sviluppo degli strumenti tecnologici nell'ambito della gestione dei lavoratori si proietta, di conseguenza, sull'esercizio del potere datoriale secondo una duplice prospettiva.
Innanzi tutto, i dispositivi digitali per la gestione dei lavoratori e per l'esecuzione della prestazione in ambienti virtuali, consentono alle imprese un maggiore accesso (quantitativo e qualitativo) ai dati dei dipendenti. In secondo luogo, si amplia la capacità di analisi dei dati acquisiti e la conseguente possibilità di accedere a nuove informazioni prima non comprensibili.

Il controllo esercitato mediante trattamenti informatizzati si modifica in ragione delle potenzialità rimesse all'elaborazione e utilizzo dei dati.
Il potere datoriale risulta, infatti, rappresentato da un nuovo e composito "potere informatico"[331] o "computazionale"[332] abilitato a elaborare i dati dei lavoratori grazie al supporto di sofisticate tecnologie informatiche.
Il controllo diviene, così, "inferenziale" ovvero basato su tecniche che fanno ricorso a metodi statistici volti a verificare le condizioni di "frequenza" dei dati analizzati.
Ciò in quanto l'elaborazione viene rimessa a sistemi algoritmici o di Intelligenza Artificiale (come *Machine Learning* o *Deep Learning*) che agiscono individuando i *pattern* (ossia regolarità) tra i dati dei lavoratori posti in correlazione.
I trattamenti inferenziali assumono, dunque, come "vere" le interazioni che si manifestano con alta ripetizione, giungendo ad attribuire a un soggetto (ossia il lavoratore) aspetti che potrebbero non caratterizzarlo.
Riscontrare una reiterazione tra correlazioni di dati non vuol dire, però, che queste siano sistematicamente vere.
Quello che ciò può determinare è la formazione di "giudizi" (o "pregiudizi") definiti *bias*[333] cognitivi, ovvero distorsioni nelle valutazioni compiute dall'analisi algoritmica.
Nella logica computazionale, propria dei sistemi di IA, il *bias* svolge una funzione fondamentale[334], definendo il *set* di supposizioni che le reti neurali impiegano per apprendere e prevedere statisticamente i risultati da *input* ignoti. Il *bias* è, così, il fondamento operativo della rete neurale su cui vengono fondate le analisi delle situazioni sconosciute.
I *bias* cognitivi vengono, in tal modo, a incidere sul potere datoriale e sul modo in cui il controllo può essere esercitato. Le caratteriste individuate dall'analisi come distintive di un individuo e qualificate come *bias* varranno, infatti, da elemento su cui esercitare il controllo e fondare le decisioni datoriali.

---

331 Cfr. Trojsi A., *Potere informatico del datore di lavoro e controllo sui lavoratori, cinquant'anni dopo*, in *dirittifondamentali.it*, n. 2, 2020, p.1414; Trojsi A., *Controllo a distanza (su impianti e strumenti di lavoro) e protezione dei dati del lavoratore*, in *Variazioni su Temi di Diritto del Lavoro*, n. 4, 2016, p. 667.
332 Cfr. Durante M., *Potere computazionale. L'impatto delle ICT*, in *Diritto società e sapere,* Meltemi, 2019.
333 Per *bias* si intende l'insieme di supposizioni per prevedere il risultato di input non ancora incontrati. Cfr. Mitchell T., *The need for biases in learning generalizations*, Rutgers University, 1980.
334 Cfr. Mitchell T., *The need for biases in learning generalization,* Rutgers University, 1980.

***

Alla luce di quanto detto, il controllo inferenziale può condurre a distinte criticità classificate dall'autrice nelle seguenti categorie in riferimento:
- al tipo di trattamento eseguito che, oltre al controllo diretto o sproporzionato sui lavoratori (di cui si è argomentato al capitolo 2) può determinare un'indagine diretta sulle opinioni dei lavoratori, una discriminazione o una profilazione anche reputazionale;
- allo strumento con cui eseguire il trattamento, con particolare riguardo alle problematiche connesse all'utilizzo di sistemi di IA.

Si procede di seguito ad analizzare brevemente le differenti criticità secondo le tipologie individuate.

2. Criticità connesse al trattamento

La maggiore quantità di informazioni accessibili e il grado di elaborazione a cui sono abilitate le nuove tecnologie apre la strada a nuovi scenari di criticità connessi all'impiego dei dati.

2.1. Indagine diretta sulle opinioni dei lavoratori

In riferimento al tipo di trattamento che può essere eseguito, le questioni interessano innanzitutto la possibilità di attuare un'indagine sulle opinioni dei lavoratori che esorbiti l'ambito d'accertamento ammesso attinente all'attitudine professionale.
Come noto, l'art. 8 SL[335] costituisce una tutela "sostanziale" all'esercizio del potere di controllo datoriale, inibendo le indagini sulle opinioni politiche, religiose o sindacali dei lavoratori e, comunque, su "*ogni fatto non rilevante ai fini della valutazione dell'attitudine professionale*".
Tale divieto ha una portata ampia, tutelando il singolo non solo in costanza del rapporto di lavoro, ma anche nella fase preassuntiva[336].
La norma statutaria ha, quindi, inteso vietare al datore di lavoro di acquisire informazioni inerenti alla sfera privata del lavoratore (o aspirante tale) ove non motivate dall'oggetto del contratto.
L'art. 8 SL intende, quindi, circoscrivere *"il rilievo della persona del lavoratore in relazione a quanto è funzionalmente collegato con la soddisfazione dell'interesse del creditore di lavoro"*[337].
Di conseguenza, risultano vietate le indagini che travalicano la valutazione di fatti oggettivamente idonei a comprovare la preparazione, la competenza, l'esperienza e la compatibilità del soggetto in relazione alle specifiche mansioni affidategli[338].

---

335 L'art. 8 SL rubricato "*Divieto di indagini sulle opinioni"* dispone che "*è fatto divieto al datore di lavoro, ai fini dell'assunzione, come nel corso dello 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".*

336 All'art. 8 SL si collega, infatti, l'art. 10 del D. Lgs. 276/2003 che ribadisce il divieto di indagini sulle opinioni o il trattamento di dati relativi a convinzioni personali, affiliazioni sindacali o politiche, al credo religioso, al sesso, all'orientamento sessuale, allo stato di famiglia, di matrimonio, di gravidanza, allo stato di salute, a eventuali handicap, alla razza o altro inerente alla condivisione d'informazioni c.d. "nuove discriminazioni" da parte di agenzie per il lavoro o altri soggetti autorizzati e accreditati.

337 Mazzotta O., *Diritto del lavoro*, Giuffrè Editore, Milano, 2011, pag. 536.

338 Pera G., *Sub art. 8,* in Assanti C., Pera G. (a cura di), *Commento allo statuto dei diritti dei lavoratori*, Cedam, Padova, 1972, pp. 108-109.

La norma ha così interrotto la prassi - precedentemente diffusa presso le grandi imprese - di compiere una "schedatura sistematica" dei dipendenti su informazioni irrilevanti alla valutazione dell'attitudine professionale, come l'affiliazione sindacale o le preferenze politiche[339].
Nota è la vicenda delle "Schedature Fiat" [340] ove l'azienda, per oltre venti anni, ha compiuto una schedatura sistematica dei propri dipendenti in riferimento alle loro opinioni in ambito soprattutto politico e sindacale. L'impresa è giunta a realizzare più di 354 mila schede relative a singoli lavoratori e riportanti tali informazioni apprese internamente agli ambienti di lavoro o al di fuori degli stessi mediante l'intervento di terzi (come le forze dell'ordine o esponenti religiosi). Gli elementi acquisiti sono stati impiegati dalla Fiat per irrogare sanzioni disciplinari o per disporre l'allontanamento dei soggetti ritenuti "pericolosi" o "sovversivi" in quanto attivi da un punto di vista politico e sindacale
Conformemente alla *ratio* dell'art. 8 SL, la giurisprudenza di legittimità[341] ha ravvisato una violazione del precetto già con la mera acquisizione dei dati afferenti a fatti od opinioni private del lavoratore, indipendentemente dal successivo utilizzo degli stessi.
La disposizione delinea, rifacendosi al lessico penalistico, un "illecito di pericolo" ove la potenzialità lesiva delle indagini datoriali giustifica *ex se* il divieto.

Le innovazioni tecnologiche e la capacità di elaborare dei dati possono, però, consentire di estrapolare informazioni personali dei lavoratori in una maniera sofisticata e, potenzialmente, idonea a eludere il divieto di cui all'art. 8 SL.
Elaborare dati "non autoevidenti" può, infatti, rendere conoscibili opinioni personali dei lavoratori, normalmente precluse al datore di lavoro, proprio grazie all'analisi e alla correlazione di dati apparentemente "neutri".
Per esempio, il crescente utilizzo di strumenti per la selezione e il reclutamene automatizzati (come gli *AST*, di cui si è parlato nel capitolo 1) basati su sistemi di *Machine Learning* che si prefiggono di individuare i candidati più idonei sulla base di informazioni contenute nei *CV* o recepite da fonti esterne, quali i *social network* (a riguardo si parla di "*social recruting*"[342]).
Tali procedimenti possono, però, consentire l'acquisizione di nuove informazioni afferenti alla sfera personale dei candidati ed eccedenti l'ambito di valutazione strettamente "professionale".
Le correlazioni sono in grado, infatti, di palesare elementi utili per una selezione, come le "*soft skill*", ma anche opinioni e tendenze dei singoli soggetti.
Tutto ciò senza che i diretti interessati ne siano a conoscenza.

La tutela statuaria manifesta, quindi, alcuni "punti deboli" quando si confronta con le capacità di analisi delle nuove tecnologie.
In primo luogo, unicamente a elaborazione avvenuta si può conoscere che tipo di informazioni siano state raccolte e, quindi, apprese dal datore di lavoro. Solo al termine dell'interpretazione, pertanto, si può comprende la vera portata dell'"indagine" compiuta.

339 Cfr. Pera G., *Sub art. 8*, in Assanti C., Pera G. (a cura di), *Commento allo statuto dei diritti dei lavoratori*, Cedam, Padova, 1972, p. 106.; Cataudella A., *Sub. art. 8*, Giuffrè Editore, Milano, 1975, pp. 236-240.
340 In merito Serra B. G., *Le schedature Fiat. Cronaca di un processo e altre cronache*, Rosenberg & Sellier, Torino,1994.
341 In tal senso Corte di Cass. n. 18302 del 19 settembre 2016, che conferma la pronuncia del Trib. Roma n. 1196 del 4/4/2013.
342 Cfr. Dagnino E., *Dalla fisica all'algoritmo: una prospettiva di analisi giuslavoristica*, ADAPT University Press, 2019, pp. 15 ss; Timellini C., *Le condotte social dei lavoratori sotto la lente della giurisprudenza*, in *Argomenti di Diritto del Lavoro (ADL)*, n. 1, 2020, pp. 286 ss.

La tutela - volta a garantire l'inaccessibilità delle informazioni non rilevanti sul piano professionale - verrebbe, così, a ridursi limitando le indagini solo in relazione alle "raccolte dei dati"[343], ma non in riferimento alle elaborazioni successive. Queste ultime potrebbero, infatti, restituire informazioni che risultano eccedenti rispetto all'ambito di indagine consentito, nonostante che i dati analizzati siano qualificati originariamente come "professionali".

Un ulteriore *vulnus* alla tutela normativa si rinviene nel caso in cui il datore di lavoro, apprese nuove informazioni grazie all'analisi condotta, decida di non impiegarle a fini decisionali.
La salvaguardia dell'art. 8 SL opera, infatti, quando il datore agisce sul piano disciplinare nei riguardi dei lavoratori con intento discriminatorio[344] sulla base delle informazioni acquisite con l'indagine (ora "analisi" dei dati).
Ove ciò non accada, la tutela risulterebbe inapplicabile, nonostante che la violazione dell'art. 8 SL si configuri nella mera acquisizione e conservazione[345] di informazioni inerenti alle opinioni personali.
In tale circostanza, inoltre, il lavoratore interessato non verrebbe mai a conoscenza che il datore di lavoro è venuto in possesso di nuovi dati particolari che lo riguardano.

Infine, l'impiego di nuove tecnologie rende sempre più effimera la portata stessa del "divieto di indagine" e di raffigurarne i limiti.
La potenzialità di analisi implementa la possibilità di accedere a nuove informazioni da parte del datore di lavoro, rendendo complesso e articolato tracciare il confine tra quelle "rilevanti", ai fini dell'attitudine professione, e quelle vietate che ineriscono la sfera individuale.

La tutela volta a garantire l'inaccessibilità alle opinioni personali sembrerebbe così ridursi, limitando la propria portata alle sole le indagini intese come "raccolte di dati" e tralasciando i risultati che possono derivare dalle analisi compiute sui dati acquisiti.
L'utilizzo di tecnologia capace di elaborare dati - mediante algoritmi o sistemi di IA – determina, quindi, il rischio che vengano occultamente indagati aspetti della vita personale posti al di fuori dei limiti tracciati dall'art. 8 SL.

2.2. Trattamenti discriminatori

L'utilizzo di dati può comportare che vengano attuati dei trattamenti discriminatori**.**
Il fenomeno della "discriminazione algoritmica"[346] è da tempo discusso in riferimento ad alcune problematiche quali la creazione di *set* di dati affetti da pregiudizi su cui effettuare l'analisi (con algoritmi)

---

[343] Cfr. Ingrao A., Donini A., *Algoritmi e lavoro*, in *Labour Law Community* del 25 maggio 2022, p. 15, consultabile *online* https://www.labourlawcommunity.org/ricerca/algoritmi-e-lavoro/ secondo le quali le analisi andrebbero limitate alle sole informazioni relative al profilo professionale, così da limitare il rischio di analisi o decisioni differenziati in ragione dei fattori protetti dell'ordinamento. In tal modo *"(…) il modello algoritmico non può essere alimentato dalle informazioni "supersensibili" di cui la norma inibisce l'indagine, ma soltanto dalle informazioni derivanti da alcune indagini (alias raccolte di dati), anche presuntive, in relazione agli aspetti "rilevanti ai fini della valutazione dell'attitudine professionale*".

[344] In merito cfr. Cataudella A., *Sub art. 8*, in Prospetti U. (a cura di) *Commentario dello Statuto dei lavoratori*, Giuffrè Editore, Milano, 1975, pp. 236 – 240; Bresciani I., *Le forme di controllo nello Statuto dei lavoratori: orientamenti giurisprudenziali e questioni di attualità,* in *Variazioni su Temi di Diritto del Lavoro*, fasc. 4, 2016, pp. 731 ss.

[345] Cfr. Corte di Cass. n. 18302 del 19 settembre 2016.

[346] Tra i tanti Barbera M, *Discriminazioni algoritmiche e forme di discriminazione*, in *Labour & Law Issues (LLI)*, vol. 7, n. 1, 2021, pp. I1 ss.; Perulli A., *La discriminazione algoritmica: brevi note introduttive a margine dell'Ordinanza del Tribunale di Bologna,* in *Lavoro Diritti Europa*, n. 1 del 14 gennaio 2021, pp. 1 ss.; Zuddas P., *Intelligenza Artificiale e discriminazioni,* in *Consulta online*, 16 marzo 2020, pp. 1-18; Pignatiello G., *Il contrasto alle discriminazioni algoritmiche*, in *Federalismi.it*, n. 16, 2021, pp. 1 ss.; Simoncini A., *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal*, n. 1, 2019, pp. 63 ss.; Tommasi S., *Algoritmi e nuove forme di discriminazione: uno sguardo al diritto europeo,* in *Revista de Direito Brasileira*, vol. 27, n. 10, 2020, pp. 112-129.

o il *training* (dei sistemi IA), la programmazione viziata dei dispositivi di analisi e il funzionamento imperscrutabile di apprendimento della tecnologia IA.
La decisione algoritmica discriminatoria può, quindi, manifestarsi perché influenzata dall'operatore umano che progetta il sistema di IA riflettendo, in tal modo, i "*preconcetti propri del programmatore o generati dai valori di riferimento dell'organizzazione in cui il programmatore opera*"[347].
Gli effetti discriminatori possono, inoltre, derivare dai *set* di dati di apprendimento apparentemente "neutri", ma in realtà viziati in quanto "inquinati" dai pregiudizi.
Infine, le discriminazioni algoritmiche possono dipendere dal modo di operare dei sistemi di IA. In questo caso, i *pattern* individuati con il processo di analisi, permettono di rivelate informazioni vulnerabili e di creare categorie in cui includere i soggetti portatori delle stesse. Il medesimo procedimento può, però, includere erroneamente nei *cluster* anche soggetti che non vi appartengano, sulla base di profili psicometrici[348] elaborati.

L'acquisizione di informazioni digitali e la successiva elaborazione comporta, quindi, una modellazione statistica *biased*[349] (ovvero basata su dati parziali) da cui possono conseguire i trattamenti "algoritmici" discriminatori[350] che possono essere classificati in: diretti, indiretti, associati, multipli o intersezionali[351].
Quelle elencate costituiscono differenti fattispecie di pregiudizio che si distinguono in base all'elemento che determina la disparità.
Nel caso della discriminazione diretta, vi è un fattore che ha effetti negativi o sfavorevoli direttamente inerenti a un soggetto. In quella indiretta, il trattamento diversificato avviene a seconda della categoria di appartenenza assegnata a un soggetto sulla base di un criterio apparentemente neutro, come definito dai Decreti Legislativi 215 e 216 del 2003**[352]**. La correlazione con il fattore pregiudizievole si costruisce, così, in ragione del divario generato da una regola di applicazione generale[353].
Nella discriminazione associata si rileva la connessione oggettiva a un fattore, a prescindere dal fatto che la vittima dello svantaggio ne sia portatrice[354], mentre con la discriminazione multipla[355] si a riferimento ad un soggetto penalizzato in base a due o più fattori discriminatori.

---

347 Zuddas P., *Intelligenza Artificiale e discriminazioni*, in *Consulta online*, 16 marzo 2020, p. 5.
348 In merito Vespignani a., Rijtano R., *L'algoritmo e l'oracolo. Come la scienza predice il futuro o ci aiuta a cambiarlo*, il Saggiatore, Milano, 2019, p. 13 parlano di "profili psicometrici" in cui si risulterebbe "ingabbiati".
349 La possibilità che sistemi di Intelligenza Artificiale ripropongano schemi pregiudizievoli a eseguendo analisi di Big Data è stata rilevata anche nell'ambito della giustizia penale digitale negli Stati Uniti, ove è stata osservata una logica discriminatoria. ciò ha portato alla creazione della *Algorithmic Justice League* (https://www.ajl.org) con la finalità di danni e pregiudizi che possono derivare dall'AI.
350 Cfr. Caruso B.- Zappalà L., *Un diritto del lavoro "tridimensionale": valori e tecniche di fronte ai mutamenti dei luoghi di lavoro*, in *WP CSDLE,* It. n. 439, 2021; Tullini P., *La salvaguardia dei diritti fondamentali della persona che lavora nella gig-economy*, in *costituzionalismo.it*, n.1, 2020, pp. 39 ss.; J. Adams- Prassl, *What If Your Boss Was an Algorithm? Economic Incentives, Legal Challenges, and the Rise of Artificial Intelligence at Work*, in *Comparative Labor Law & Policy Journal 123,* vol. 41, n. 1, 2019, pp. 1 ss.; Giacomelli L., *Big brother is «*gendering*» you. Il diritto antidiscriminatorio alla prova dell'intelligenza artificiale: quale tutela per il corpo digitale?*, in *BioLaw Journal*, n. 2, 2019, pp. 269 ss.;.; V. Maio, *Il diritto del lavoro e le nuove sfide della rivoluzione robotica*, in *Argomenti di Diritto del Lavoro* (*ADL)*, n. 6, 2018, pp. 1414 ss; Peruzzi M., *Il diritto antidiscriminatorio al test di intelligenza artificiale*, in *Labour & Law Issues (LLI)*, vol. 7, n.1, 2021, pp. I49 ss.
351 Cfr. Peruzzi M., *Il diritto antidiscriminatorio al test di intelligenza artificiale*, in *Labour & Law Issues (LLI)*, vol. 7, n.1, 2021, p. I56.
352 Dagnino E., *People analytics: lavoro e tutele al tempo del management tramite big data*, in *Labor & Law Issues (LLI)*, vol. 3, n. 1, 2017, p. 23.
353 Ovvero un trattamento diversificato a seconda della categoria assegnata sulla base ad un criterio apparentemente neutro, così come definito dai Decreti Legislativi 215 e 216 del 2003. Cfr. Dagnino E., *People analytics: lavoro e tutele al tempo del management tramite big data*, in *Labor & Law Issue (LLI)*, vol. 3, n. 1, 2017, p. 23.
354 Cfr. Corte giust. 17 luglio 2008, C-303/06, *Coleman*; Corte giust. 16 luglio 2015, C- 83/14, *Chez*.
355 Cfr. Carnovali S., *Profili delle politiche nazionali ed europee di contrasto alle discriminazioni multiple*, Rivista del Gruppo di Pisa consultabile su: https://www.gruppodipisa.it/images/rivista/pdf/Sara_Carnovali_-_Profili_delle_politiche_nazionali_ed_europee_di_contrasto_alle_discriminazioni_multiple.pdf.

Infine, la discriminazione intersezionale si manifesta quando la disparità di trattamento è fondata sulla combinazione di più fattori che agiscono tra loro in modo inscindibile[356].

La possibilità di attuare un trattamento discriminatorio qualificato come indiretto è un'ipotesi che si è già concretizzata sia mediante l'impiego di sistemi di Intelligenza Artificiale, sia ricorrendo ad algoritmi.
In riferimento all'impiego di un sistema di IA "discriminatorio", il caso è quello della multinazionale Amazon[357] che, nel 2018, aveva predisposto un processo automatico di selezione dei migliori candidati basato su un dispositivo *AST* che analizzava i *CV* mediante *Text Mining*.
Osservando l'operatività del processo di selezione si è constatato che il sistema di IA operava in maniera "discriminatoria"[358] selezionando in modo statisticamente rilevante candidati esclusivamente di sesso maschile.
Il sistema, basato su una logica di *Machine Learning*, era stato allenato fornendo i *Curricula Vitae* dei candidati scelti nella decade precedente e opportunamente anonimizzati, anche in riferimento al genere.
Nonostante ciò, il sistema di IA aveva agito riproducendo i medesimi criteri di valutazione (e di preferenza) espressi dai valutatori. In che maniera? Ricercando all'interno dei *CV* gli elementi ritenuti "forti" e, dunque, "veri" secondo la logica statistica.
Il sistema di IA è, quindi, riuscito a individuare nei *Curricula* elementi apparentemente "neutri" (quali avverbi adoperati nella presentazione o corsi universitari frequentati) rivelatisi distintivi e caratterizzanti i candidati maschi. Per tale ragione, questi fattori venivano valutarti come "forti" e i *CV* in cui erano presenti da preferirsi ad altri.
La presenza di tali elementi all'interno dei CV è stato, quindi, il criterio adottato dal sistema di IA per compiere la "miglior selezione" dei candidati.
Casi analoghi, in cui sono stati preferiti soggetti di sesso maschile a dispetto di quello femminile, si sono verificati anche presso altre società quali *Uber*[359] e *LinkedIn*[360].

Di "discriminazioni multiple" in generale si parla anche in documenti non vincolanti (*soft law*) del Parlamento europeo, come ad esempio la Risoluzione sulla situazione di donne appartenenti a gruppi minoritari nell'Unione europea (2003/2109(INI)), che si concentra sulle donne disabili, migranti e rom. Sempre in riferimento alle discriminazioni multiple riguardanti le donne rom. Cfr. European Parliament, 2009. *Resolution of 11 March 2009 on the social situation of the Roma and their improved access to the labour market in the EU* P6_TA(2009)0117. Available at: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P6- TA-20090117.

356 Ad esempio, il binomio "donne black" o "donne rom". Cfr. Militello M. – Strazzari D., *I fattori di discriminazione*, in M. Barbera - A. Guariso (a cura di), *La tutela antidiscriminatoria*, Giappichelli Editore, Torino, 2019, 85 ss.

357 L'11 ottobre 2018 viene pubblicato da Reuters l'articolo "*Amazon scraps secret AI recruiting tool that showed bias against women*" https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G. Caso ripreso anche da G. Gaudio, *Algorithmic management, poteri datoriali e oneri della prova: alla ricerca della verità materiale che si cela dietro l'algoritmo* in *Labour & Law Issues (LLI)*, vol.6, n. 2. 2020, pp. 46, 46. Per ulteriori approfondimenti sulla tematica si rinvia a Kullmann M., *Discriminating job* applicants *through algorithmic decision-making,* in SSRN, 1 gennaio 2019, consultabile *online* https://ssrn.com/abstract=3373533; Hacker P., *Teaching fairness to artificial intelligence: existing and novel strategies against algorithmic discrimination under EU law,* in *55 Common Market Law Review*, 2018; Gaudio G., *Algorithmic management, sindacato e tutela giurisdizionale*, *in Diritto delle Relazioni Industriali,* n. 1, 2022, pp. 30 ss.

358 Nardocci C., *Intelligenza artificiale e discriminazion*e, in atti del Convegno annuale Associazione Gruppo di Pisa "*Il diritto costituzionale e le sfide dell'innovazione tecnologica",* Genova 18/19 giugno 2021.

359 Cfr. Melendez S., *Uber driver troubles raise concerns about transgender face recognition*, 8.9.2018*,* consultabile su *https://www.fastcompany.com/90216258/uber-face-recognition-tool-has-locked-out-some-transgender-drivers.*

360 Cfr. Cooney S., *LinkedIn Tweaks Search Algorithm After Report Suggests Gender Bias*, 8.9.2016, consultabile su https://time.com/4484530/linkedin-gender-bias-search/.

Senza rivolgere lo sguardo oltre oceano recentemente anche il Tribunale di Bologna, nell'ordinanza del 31.12.2020[361], ha riconosciuto la sussistenza di una discriminazione indiretta attuata, mediante un algoritmo, dalla società *Deliveroo* nei confronti dei *rider* impiegati per le consegne.
Secondo il Tribunale il sistema di profilazione adottato dalla piattaforma, basato sul parametro di "affidabilità" dei *rider* e calcolato in maniera direttamente proporzionale al grado di "disponibilità" garantito, non era capace di distinguere chi si assentava in ragione di una preferenza personale da chi agiva per legittimi interessi (come esercitare il diritto di sciopero o mancare per infortunio o malattia).
L'algoritmo nominato "Frank" classificava tutti i lavoratori assenti indistintamente come "non affidabili". Qualifica, quest'ultima, che riduceva significativamente le opportunità di lavoro, escludendo i lavoratori "inaffidabili" dalle fasce di lavoro maggiormente remunerative o dalle zone più ambite.
L'algoritmo, pertanto, classificando i *rider* in maniera indistinta in base al parametro "assenza", agiva compiendo una discriminazione indiretta.

Un esempio di una discriminazione compiuta mediante fattori associati si rinviene, invece, nella pronuncia della Corte di Giustizia dell'Unione Europea nella sentenza del 16 luglio 2015 della causa C-83/145 (Chez Razpredelenie Bulgaria).
La vicenda ha preso avvio dal ricorso presentato dalla signora Nikolova, proprietaria di un negozio di alimentari nel quartiere di «Gizdova mahala» nella città di Dupnitsa (Bulgaria), che lamentava l'impossibilità di accedere al proprio contatore di energia posto a un'altezza inaccessibile di 6/7 metri da terra.
L'installazione del contatore a tale altezza era determinata al fatto che nel quartiere di «Gizdova mahala» era presente un'ampia rappresentanza di bulgari di origine *rom*. Rappresentanza a cui non apparteneva la ricorrente.
Per tale motivo, però, la CHEZ RB, impresa di distribuzione di energia elettrica, aveva apposto i contatori elettrici sui pali di cemento a un'altezza di 6 o 7 metri, al fine di limitare i casi di manomissione e di allacciamento illegale. Fenomeni che si manifestavano con maggior frequenza nelle aree con prevalente popolazione di origine *rom*.
Differentemente, negli altri quartieri della città (in cui i *rom* non costituivano la maggioranza) i contatori installati venivano collocati a un'altezza di 1,70 metri presso la residenza degli utenti.
La Corte, nella propria pronuncia, ha riconosciuto che l'azienda aveva attuato un trattamento sfavorevole sproporzionato rispetto ai residenti del quartiere sulla base di un pregiudizio legato all'origine etnica degli stessi.
Caratteristica che, però, che non apparteneva alla signora. Nikolova di cui aveva comunque patito gli effetti negativi in forza di una discriminazione associata.

---

[361] Per un'analisi dell'ordinanza si rinvia *ex multis* a Perulli A., *La discriminazione algoritmica: brevi note introduttive a margine dell'Ordinanza del Tribunale di Bologna*, in *Lavoro Diritti Europa*, n. 1, 2021; Ballestrero M. V., *Ancora sui rider. La cecità discriminatoria della piattaforma*, in *Labor*, n. 1, 2021, pp. 104 ss; Peruzzi M., *Il diritto antidiscriminatorio al test di intelligenza artificiale,* in *Labour & Law Issues (LLI),* vol. 7, n. 1, 2021, pp I49 ss; Santagata De Castro R., *Anti- discrimination Law in the Italian Courts: the new frontiers ofthe topic in the age ofalgorithms*, in Biblioteca '20 Maggio', n. 1, 2021 (originariamente pubblicato in *WP CSDLE,* It. n. 440, 2021), pp. 193 ss.; Faioli M., *Discriminazioni digitali e tutela giudiziaria su iniziativa delle organizzazioni sindacali*, in *Diritto delle Relazioni Industriali* (*DRI)*, n. 1, 2021, pp. 204 ss.; Ingrao A., *Riflessioni intorno alla partecipazione dei lavoratori nell'era dell'algoritmo, alla luce dell'accordo Just Eat- Takeaway.com*, in Mingione E., Scarpelli F., Giasanti L. (a cura di), *Lo Statuto dei lavoratori alla prova dell'oggi: Una rilettura critica da parte degli studiosi di nuova generazione,* Feltrinelli, Milano, 2022*, pp 118 ss.* Consultabile al *link: https://fondazionefeltrinelli.it/app/uploads/2022/11/Finale_StatutoLavoratori-1.pdf.*; Ingrao A, *I sistemi di feedback basati su rating e reviews tra controllo della prestazione lavorativa e divieto di decisioni automatizzate*, in C. Alessi, M. Barbera, L. Guaglianone (a cura di) in *Impresa, lavoro e non lavoro nell'economia digitale*, 2019, Bari, Cacucci, pp. 203 ss.

Parimenti, nella causa C-303/06 (*Coleman / Attridge Law e Steve Law*), con sentenza il 17 luglio 2008, la Corte di Giustizia dell'Unione Europea ha riconosciuto che il trattamento meno favorevole patito dalla signora Coleman, lavoratrice presso studio legale, era stato determinato da una discriminazione associata. La ricorrente aveva dovuto, infatti, rassegnare le proprie dimissioni in quanto madre di un figlio disabile e avendo visto negare le proprie richieste, avanzate per tale motivo, di ottenere una maggiore flessibilità nell'orario di lavoro.
La Corte, pronunciandosi in merito, ha dichiarato come nei confronti della lavoratrice era stata esercitata una discriminazione in relazione alla disabilità di cui era affetto il figlio.
Il pregiudizio era, dunque, associato all'invalidità di un altro soggetto.

In entrambi i casi, la discriminazione era stata dettata da un operato umano.
Ciò che preme evidenziare è come la capacità di elaborare dati, la cui analisi si basa sull'individuazione di *pattern* di correlazione, rende possibile e - da un certo punto di vista - maggiormente accessibile realizzare una "discriminazione associata".
L'attività di elaborazione inferenziale dei sistemi algoritmici e di IA incrementa, infatti, la possibilità di creare associazioni tra soggetti apparentemente irrelati.

La capacità di analizzare ed estrarre informazioni accresce anche l'opportunità di conseguire discriminazioni multiple o inferenziali, ovvero di attuare quei trattamenti pregiudizievoli basati su più fattori selettivi tra loro connessi.
Per esempio, la discriminazione in base all'età è stata sempre considerata come fattore indipendente rispetto ai pregiudizi connessi alla disabilità.
Nell'ambito lavorativo i soggetti più anziani sono stati talvolta penalizzati in quanto considerati uno "svantaggio competitivo" per l'organizzazione[362].
Alcuni studi[363] hanno, però, dimostrato che sussiste un forte legame tra i due fattori (età e disabilità) rilevando come un soggetto, all'aumentare degli anni, incrementi anche la possibilità di manifestare condizioni inabilitanti (connesse ad alcune patologie come ictus o malattie cardiovascolari).
Ciò può determinare la possibilità che vengano messe in atto discriminazioni multiple o inferenziali (ponendo in relazione età e disabilità) o associate (collegando l'età di una persona al suo stato di salute, anche se quest'ultima non è portatrice di alcun *handicap).*
Disparità di trattamento che possono essere attuate con maggior accessibilità mediante l'analisi dei dati che consentono di acquisire nuove informazioni apparentemente incongrue.

Volendo categorizzare le cause che possono determinare una situazione discriminatoria mediante l'utilizzo di sistemi algoritmici, queste possono essere ricondotte a differenti fattori, quali:

1. "discriminazione intenzionale", celata dietro una programmazione viziata, volutamente architettata con intenti pregiudizievoli verso determinate categorie di soggetti.
2. *Training* viziato dei sistemi di IA, basati su *set* di dati costruiti su giudizi passati di natura discriminatoria.

[362] Bersin J., Chamorro-Premuzic T., *The case for hiring older workers*, in *Harvard Business Review* consultabile *online* https://hbr.org/2019/09/the-case-for-hiring-older-workers.
[363] Equality and Human Rights Commission, *Disability Discrimination*, consultabile *online* www.equalityhumanrights.com/en/advice-and-guidance/disability-discrimination; Spencer J., *Age and Disability Discrimination & Your Rights*, su Jackson Spencer Law del 5 Mar. 2020, consultabile *online* https://jacksonspencerlaw.com/age-and-disability-discrimination/

3. Elaborazione di un "*proxy*" o dato alternativo[364], su cui basare l'analisi, che risulti fallato o errato. In questo caso, lo scopo perseguito dal sistema di IA è legittimo, ma ne risulta alterato il criterio di valutazione.
   Per esempio, se si vuole prevedere la "capacità lavorativa" di un candidato, non esistendo un criterio obiettivo che la rappresenti, questa può essere desunta sulla base di altri elementi che si presume esserne rappresentativi: come le ore lavorate o la presenza in orario sul luogo di lavoro. Entrambi i criteri si possono, però, rivelare discriminatori.
   Il primo, inerente alle ore lavorate, potrebbe penalizzare le candidate di sesso femminile, portate tradizionalmente a trascorrere meno tempo in ufficio per assolvere impegni di natura familiare, nonostante la produttività sia la medesima dei colleghi di sesso maschile.
   Il secondo criterio, relativo alla "puntualità", potrebbe celare un pregiudizio di classe, andando a discapito di coloro che appartengono ad una fascia sociale inferiore e, per tale ragione, portati a vivere in zone periferiche più vantaggiose da un punto di vista economico[365].
4. Selezione delle caratteristiche rilevanti per elaborare un modello algoritmico di analisi.
   Il sistema di IA potrebbe, in questo caso, operare in modo discriminatorio tenendo in considerazione alcune caratteristiche connesse all'obiettivo che si intende raggiungere, come selezionare il "miglior candidato", ma applicando tali criteri solo ad alcune categorie di persone.
   Per esempio, alcuni sistemi automatici di assunzioni operano assegnando un punteggio elevato ai candidati che hanno frequentato scuole di *elite* e possiedono un diploma definito *ivy-league*[366]. Tale criterio si può rivelare discriminatorio nei confronti di chi, pur non avendo frequentato scuole di "alto livello" (e contestuale "costo elevato"), vantano una preparazione analoga. Dato che può essere desunto dai voti ottenuti nelle materie di esame sostenute.
   Anche in questo caso, verrebbe compiuta una discriminazione associata alla classe socioeconomica di appartenenza.
   Un'altra causa di discriminazione connessa a tale problematica può essere ravvisata nella circostanza che la registrazione dei dati da analizzare non rifletta la frequenza con cui i fenomeni si manifestano.
   Il caso potrebbe essere, per esempio, quello dei controlli a cui gli appartenenti a differenti etnie possono essere soggetti da parte delle forze dell'ordine.
   Nel caso in cui un'etnia sia soggetta a verifiche in misura maggiore rispetto ad un'altra, il sistema di IA effettuerà l'analisi non sulla base dei dati reali, ma sulla base di quelli immessi nel *set* di dati posto a *training*.
   Il sistema potrebbe, quindi, indicare che determinati reati vengano effettuati con maggior frequenza da un gruppo etnico rispetto ad un altro poiché, sulla base dei dati parziali immessi, associa che, chi appartiene al gruppo sociale più controllato, è portato e tenere un comportamento criminoso.

---

364 Barocas S, Selbst A. D., *Big Data's Disparate Impact*, in *California Law Review*, vol. 104, n. 671, 2016, pp. 677 – 680; McKenzie R., *Bots, Bias and Big Data: Artificial Intelligence, Algorithmic Bias and Disparate Impact Liability in Hiring Practices*, in *Arkansas Law Review,* vol. 71, n. 2, 2018, pp. 529 ss. L'autore a pagina 534 osserva che "*Essentially, what makes a 'good' employee must be defined in ways that correspond to measurable outcomes*".

365 Kanoogo Y., *Addressing Bias in HR Algorithms*, in Medium (Mar. 18, 2020), consultabile *online* https://medium.com/@yashkanoongo/addressing-bias-in-hr-algorithms-2b0f9003ed64.

366 Barocas S, Selbst A. D., *Big Data's Disparate Impact*, in *California Law Review*, vol. 104, n. 671, 2016 pp. 677- 680; The New York Times, *We need laws to take on racism and sexixm in hiring technology*, consultabile *online* https://www.nytimes.com/2021/03/17/opinion/ai-employment-bias-nyc.html

Allo stesso modo, il progetto "The Coded Gaze"[367], ha rivelato come i dati di *training* in cui le donne di colore sono sottorappresentate ha portano alcuni *software* di riconoscimento facciale, basati su un sistema di *Machine Learning*, a essere meno performanti nel riconoscere i volti delle donne nere rispetto ai volti di donne bianche.

5. I sistemi di IA possono, inoltre, imparare da esempi passati senza tenere conto che ci possono essere delle evoluzioni nel comportamento sociale. Il *training* potrebbe, quindi, non rappresentare adeguatamente le variazioni intercorse.
   Per esempio, si è verificato il fenomeno di proporre con maggior frequenza annunci di posizioni manageriali a uomini o, comunque, a soggetti facenti parte di una "maggioranza"[368].
   Ciò sulla base di condizioni passate ove donne o "minoranze" non avevano assunto posizioni direttive.
   In forza di ciò, il sistema riteneva che i soggetti "meno rappresentati" non avessero interesse a ricoprire tali cariche.
   La questione si connette al problema della "sotto-rappresentanza" di un gruppo, ovvero alle discriminazioni che possono attuarsi quando sono presenti pochi esempi all'interno di un *set* di dati (es. donne in posizione apicale).
   In questo caso il sistema di IA può non associare come idonee le donne ad assumere posizioni apicali perché non vi è un campione sufficientemente rappresentativo.
   Una classe di persone può, quindi, essere considerata non qualificata e automaticamente rifiutata dal sistema di IA nella valutazione oppure il sistema potrebbe proporre una determinata posizione solo ad alcuni soggetti ritenuti "idonei".
   Questo è quanto accaduto nel 2019 con gli annunci di reclutamento sul *social* Facebook che proponeva la posizione di cassiera ad un pubblico composto per 85% da donne, mentre la pubblicità per ricoprire il ruolo di tassista venivano mostrate a soggetti appartenenti per il 75% a comunità straniere[369].
   La mancanza di rappresentanza di alcuni gruppi di popolazioni porta l'algoritmo a "non vederle", ritenendole irrilevanti[370].
6. Infine, le discriminazioni possono derivare da "codifiche ridondanti" o "*redundant encodings*"[371] ovvero casi in cui l'appartenenza a una classe protetta è codificata in altri dati. Ciò si verifica quando un particolare dato (o determinati valori per quel dato) è altamente correlato con l'appartenenza a specifiche classi protette. L'esempio potrebbe essere l'impiego di dati comuni relativi, per esempio, alla residenza per identificare dati particolari come l'origine etnica[372].

L'enorme potenziale per l'IA nell'analizzare dati ed estrarre nuove informazioni può, dunque, perpetuare o addirittura esacerbare i pregiudizi già esistenti attuati da operatori umani.

---

[367] Cfr. The Coded Gaze: https://www.ajlunited.org/the-coded-gaze. In merito anche Buolamwini J., Gebru T., *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, in Proceedings of Machine Learning Research, vol. 81, 2018, pp. 77 – 91, consultabile *online* http://proceedings.mlr.press/v81/buolamwini18a.html?mod=article_inline.

[368] Bogen M., *All the Ways Hiring Algorithms Can Introduce Bias*, in *Harvard Business Review*, May 2019, consultabile *online* https://hbr.org/2019/05/all-the-ways-hiring-algorithms-can-introduce-bias.

[369] Bogen M., *All the Ways Hiring Algorithms Can Introduce Bias*, in *Harvard Business* Review, May 2019, consultabile *online* https://hbr.org/2019/05/all-the-ways-hiring-algorithms-can-introduce-bias.

[370] Lo studio "Gender Shades" rivela come alcuni dei i *set* di dati scelti per addestrare i dispositivi di riconoscimento facciale sono distorti, come nel caso di un *set* di dati di volti di celebrità contenenti il 77,5% di volti maschili e l'83,5% di volti bianchi. Ciò ha determinato una *performance* nettamente inferire rispetto alle categorie di popolazione sottorappresentate.

[371] Barocas S, Selbst A. D., *Big Data's Disparate Impact*, in *California Law Review*, vol. 104, n. 671, 2016, pp. 691 -692.

[372] Come avvenuto della Corte di Giustizia dell'Unione Europea nella sentenza del 16 luglio 2015 della causa C-83/145 (Chez Razpredelenie Bulgaria), prima analizzata.

Elaborare i dati impiegando tecniche avanzate incrementa, infatti, le *chances* di identificare elementi che possono rivelarsi distorti per classificare, sotto un'apparente etichetta di obiettività, soggetti come appartenenti a determinate categorie.

2.3. Profilazione (rinvio)

L'utilizzo di sistemi automatici di *Data Mining* può comportare l'esecuzione di un trattamento di profilazione[373], anche reputazionale.

Come si approfondirà nel capitolo successivo, la capacità di elaborare dei sistemi di *Data Analytics* può, infatti, concludersi con l'attribuzione di un punteggio (analisi *net promoter score*) che consenta di classificare le parole chiave individuate o i comportamenti definiti.

L'utilizzo di tecniche analitiche per l'individuazione di *pattern* di classificazione, basati anche su aspetti personali, integra l'ipotesi di profilazione, come descritta dall'art. 4 del Regolamento 2016/679 (GDPR).

La disposizione fondamentale prevista dal GDPR sulle decisioni automatizzate è l'art. 22[374] che vieta l'utilizzo, salvo tassative eccezioni, di processi completamente automatizzati che comportano effetti legali o conseguenze significative per l'interessato.

Il Gruppo di lavoro WP29[375] ha chiarito che l'interpretazione deve essere intesa in senso ampio, precisando che un processo è e rimane completamente automatizzato anche ove vi sia un coinvolgimento umano, ma di entità marginale rispetto all'intervento automatico.

La profilazione può avvenire, inoltre, in base a giudizi espressi sull'interessato, come avviene per *Uber*[376] mediante *feedback* e "*rating and reviews*"[377] degli utenti, oppure elaborando un profilo reputazionale, come accaduto con la piattaforma *web* Mevaluate. Quest'ultima elaborava un *rating* degli iscritti sulla base di elementi "*rilevati anche sotto il profilo etico*" [378] per la selezione delle controparti negoziali, tra cui figuravano anche "*aspiranti dipendenti*" e "*dipendenti in forza*".

Si deve, infine, tenere in considerazione l'inefficacia del consenso eventualmente espresso dal dipendente per l'esecuzione di tali trattamenti (non strettamente connessi al contratto di lavoro o previsti per legge) in ragione della condizione di "vulnerabilità" riconosciuta verso il datore di lavoro.

Il consenso fornito sarebbe, dunque, viziato in quanto privo del requisito della libertà di espressione posto che il diniego "*potrebbe causare allo stesso* (ndr. dipendente) *un pregiudizio reale o potenziale*"[379].

---

373 Art. 4 GDPR: la profilazione è qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali 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.

374 Art. 22 parg. 1 del GDPR garantisce il diritto dell'interessato a "*non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici he lo riguardano o che incida in modo analogo significativamente sulla persona*".

375 Gruppo di Lavoro WP29, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (17/EN WP251rev.01).

376La piattaforma Uber spiega così il sistema di *feedback* adottato: https://www.uber.com/it/it/drive/basics/how-ratings-work/#:~:text=La%20piattaforma%20Uber%20utilizza%20un,Cerchi%20informazioni%20sulle%20consegne%3F.

377 A riguardo Ingrao A., *I sistemi di feedback basati su rating e reviews tra controllo della prestazione lavorativa e divieto di decisioni automatizzate*, in Alessi C., Barbera M., Guaglianone L. (a cura di), *Impresa, lavoro e non lavoro nell'economia digitale*, Cacucci Editore, Bari, 2019, pp. 193 ss.

378 Provvedimento del Garante per la Protezione dei Dati Personali del 24.11.2016 "*piattaforma web per l'elaborazione di profili reputazionali"* punto 1.2 secondo capoverso.

379 Opinione 2/2019 dell'European Data Protection Board (ex WP29).

2.4. Controllo "tecnologico" diretto (rinvio)

Infine, come argomentato nel capitolo 2, l'elaborazione dei dati può consentire al datore di lavoro di compiere un controllo "tecnologico" diretto della prestazione lavorativa e, in quanto tale, vietato ai sensi dell'art. 4 co. 1 SL.

Tale ipotesi può ricorrere soprattutto quando i dati risultano "non strutturati" o "*exhaust data*", ovvero quando l'elaborazione algoritmica si dimostra preponderante. La mancata conoscenza *ab origine* del significato e della finalità di trattamento può determinare, a seguito dell'elaborazione, l'acquisizione di informazioni eccedenti le finalità individuate dall'art. 4 SL. Informazioni che, una volta conosciute dal datore di lavoro, potrebbero consentire un controllo diretto del lavoratore, al di fuori delle esigenze normativamente ammesse.

3. Criticità inerenti allo strumento con cui si esegue il trattamento

Come si è anticipato, anche l'utilizzo di sistemi di IA a supporto dell'attività di elaborazione dei dati non è esente da criticità.

Queste interessano, in primo luogo, la necessità di fornire ai sistemi grandi quantità di "*training data*" che devono al contempo possedere un'elevata qualità. Ciò porta ad acquisire enormi volumi di dati (relativi ai lavoratori) che siano il più possibile accurati.

Un altro problema è quello dell'*overfitting*, ovvero la circostanza per cui un sistema di IA possa divenire talmente accurato nell'elaborazione di dati che le sue previsioni non risultino più efficaci quando si trova ad analizzare nuovi esempi di portata più generale.

L'utilizzo di tecniche di IA può, inoltre, comportare il pericolo di fenomeni "*flash crashs"*, ovvero di quella circostanza *"in cui due algoritmi interagiscono generando conseguenze imprevedibili"*[380], o un "*bias* di automazione"[381] che descrive lo stato di dipendenza dell'operatore dalla tecnologia e la tendenza a favorire decisioni elaborate da sistemi automatici, ignorando dati o decisioni umane contrarie.

La criticità che viene, però, maggiormente contestata dalla dottrina sull'utilizzo di tecniche IA di *Machine Learning e Deep Learning* è la mancata trasparenza nel funzionamento[382], tanto da definire questi sistemi delle "*black box*"[383].

Anche quando, infatti, i sistemi di IA mostrano risultati eccellenti nella loro elaborazione, risulta impossibile spiegarne le basi tecniche e logiche delle decisioni assunte. Vi è, quindi, conoscenza degli *input* (ovvero dei dati immessi) e degli *output* (ossia dei risultati elaborati), ma non dei processi intermedi. Ciò rende impossibile giustificarne in maniera trasparente e univoca le analisi e i processi decisionali operati.

L'opacità operativa di un sistema di IA risiede nella sua architettura, costituita da una rete neurale convoluzionale, che genera una asimmetria cognitiva tra soggetto interessato e utilizzatore, data anche dalla complessità tecnica che la rende difficilmente intellegibile.

Un sistema di reti neurali, infatti, elabora soluzioni sulla base di una soppesata gerarchica di dati, ma non è in grado di restituire il motivo delle decisioni assunte, né di condividere le regole poste alla base del ragionamento compiuto.

L'opacità della rete è ravvisabile anche nel processo di apprendimento automatico, caratterizzato da imprevedibilità e non intenzionalità.

---

380 Proposta per una Strategia Italiana per l'Intelligenza Artificiale elaborata dal Gruppo di Esperti MISE sull'Intelligenza Artificiale del 2 luglio 2020, p. 18.

381 Wickens C.D, Clegg B.A., Vieane A.Z, Sebok A.L., *Complacency and Automation Bias in the Use of Imperfect Automation*, in *Human factors*, vol. 57, n. 5, 2015, pp. 728 – 739.

382 Adams-Prassl J., *What if your boss was an algorithm?*, in *Comparative Labor Law & Policy Journal 123*, vol. 41, n. 1, 2019, pp. 1-30.

383 In merito Pasquale F., *The black box society: the secret algorithms that control money and information*, Cambridge Mass., Harvard University Press, London, 2016.

Apprendimento che può risultare viziato ove compiuto su un *set* di dati alterato, come avvenuto nel 2018 con il sistema AI di reclutamento elaborato da Amazon[384].

Un sistema neurale può, dunque, celare anche un'opacità "intenzionale" ove il *training* sia volutamente compiuto su dati condizionati da fattori sociali e valori morali di chi ha assunto le decisioni precedenti, poste a modelli di apprendimento.
Con il risultato di esercitare un controllo inferenziale che può avere effetti discriminatori.

Tali caratteristiche hanno, quindi, portato la dottrina a definire i sistemi di IA quali "*black box*"[385] volendo così sottolineare l'asimmetria informativa tra interessati (lavoratori) e titolare del trattamento (datore di lavoro) che accentuerebbe lo squilibrio di poteri già presente nel rapporto di lavoro.
Disequilibrio informativo che diverrebbe particolarmente problematico in quanto la mancata trasparenza del procedimento renderebbe difficile (se non impossibile) mettere in discussione le decisioni assunte dal datore di lavoro "automatizzato"[386].
Infine, da alcuni autori viene sottolineata la profonda influenza che i sistemi di IA hanno la cui pervasività risiederebbe nel fatto che essi vengano impiegati con intensità crescente e che gli ambienti sociali si stiano trasformando al fine di favorirne la diffusione[387].
Esempio ne è proprio la gestione dei rapporti di lavoro strettamente connessa alla digitalizzazione e datificazione dello stesso.
Preoccupazione che vorrebbe scongiurare di giungere a una "dittatura dell'algoritmo"[388] ove "*lo sviluppo dell'automazione porti l'uomo in una posizione di subordinazione a una sua stessa creazione*"[389].

4. La normativa applicabile

Le criticità descritte non trovano soluzione in una disciplina organica, mancando una normativa specifica che regoli l'utilizzo di tecniche di *Data Analyst*.
L'interprete, pertanto, in una prospettiva *de jure condendo*, è chiamato a individuare quali norme del diritto nazionale e internazionale risultino adeguate alla fattispecie.
Per affrontare in modo consapevole le potenzialità e i rischi insiti all'attività di *Data Analyst* è, quindi, necessario un attento studio comparato della normativa vigente in ambiti affini di tutela.

---

384 L'11 ottobre 2018 viene pubblicato da Reuters l'articolo "*Amazon scraps secret AI recruiting tool that showed bias against women*" https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G. Caso ripreso anche da G. Gaudio, *Algorithmic management, poteri datoriali e oneri della prova: alla ricerca della verità materiale che si cela dietro l'algoritmo* in *Labour & Law Issues (LLI)*, vol.6, n. 2. 2020, pp. 46, 46.

385 Adam-Prassl J.*, A thematic working paper for the annual conference of the European Centre of Expertise (ECE) in the field of labour law, employment and labour market policies: exploring ways to improve working conditions of platform workers: the role of EU labour law. Algorithmic management and the EU social acquis: opening the black box*, october 2020.

386 A riguardo Jeremias Adam-Prassl "*the granularity and intensity of Control exercised through algorithmic management, finally, is particular problematic given a consistent lack of transparency, from the inception of the employment relationship all the way through to its suspension or termination, and the concomitant difficulties in challenging automated or algorithmically informed employer decisions".* Adam-Prassl J.*, A thematic working paper for the annual conference of the European Centre of Expertise (ECE) in the field of labour law, employment and labour market policies: exploring ways to improve working conditions of platform workers: the role of EU labour law. Algorithmic management and the EU social acquis: opening the black box*, october 2020, p. 5.

387 In merito Durante M., *Potere computazionale. L'impatto delle ICT* in *Diritto, società, sapere*, Meltemi, 2019. L'autore osserva come la riconfigurazione dell'ambiente dovuta agli algoritmi comporti "*quella epistemica della conoscenza e della rappresentazione del mondo*" (p. 37).

388 Rodotà S., *Il mondo nella rete. Quali i diritti, quali i vincoli*, Laterza, Roma-Bari, 2014, pp. 33 ss. In merito anche Molaschi V., *Algoritmi e nuove schiavitù*, in *Federalismi.it*, n. 18, 2021, pp. 205 ss che fa riferimento a un "dominio dispotico" degli algoritmi.

389 Pajno A., Bassini M.,De Gregorio G., Macchia M., Patti F. P.., Pollicino O., Quattrocolo S., Simeoli D., Sirena P., *AI: profili giuridici. Intelligenza artificiale: criticità emergenti e sfide per il giurista*, in *BioLaw Journal*, n. 3, 2019, p. 13.

Criteri orientativi possono essere desunti nelle fonti dettate per la tutela dei dati personali, sui *Big Data*, sull'Intelligenza Artificiale, sulla gestione algoritmica e nel diritto del lavoro.
Non potranno, inoltre, essere trascurati i diritti fondamentali della persona e, nello specifico, dei lavoratori che si articolano sviluppando i concetti di dignità della persona, non discriminazione e protezione della vita privata.
La tutela dei diritti fondamentali è certamente sancita a livello europeo dalla Carta dei Diritti Fondamentali dell'Unione Europea[390] e dalla Costituzione italiana, programmaticamente orientata a tutelare il lavoratore come soggetto debole del rapporto di lavoro[391].
L'impatto delle attività imprenditoriali sui diritti umani e sul loro rispetto è stato oggetto di studio da parte del Consiglio per i diritti umani delle Nazioni Unite che nel 2011 ha redatto dei Principi Guida su Impresa e Diritti Umani[392].
Tali Principi rappresentano uno strumento di "*soft law*" che, pur non producendo effetti giuridici vincolanti, formano il quadro di riferimento per lo sviluppo di piani d'azione a livello nazionale.
In forza di ciò, nel dicembre 2016 l'Italia ha adottato il "Piano di Azione Nazionale su Impresa e Diritti Umani" (PAN) per il periodo 2016-2021[393] che intende contrastare le distorsioni che possono derivare dall'attività d'impresa sui diritti umani al fine di "*migliorarne la protezione, ma anche per assicurarne un più alto livello di tutela attraverso lo sviluppo di un'adeguata cultura imprenditoriale e di nuove opportunità di crescita economica all'interno di un sistema di sana e corretta competizione economica*"[394].

La crescente osservabilità del lavoro determina la necessità di analizzare le norme vigenti in ambito *privacy*.
La tutela dei dati personali[395] nel diritto europeo trova fondamento nel Trattato sul Funzionamento dell'Unione Europea e nel Trattato sull'Unione Europea prevedendo il primo che "*il Parlamento europeo e il Consiglio (...) stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale (…)*" (art. 16) e il secondo che *"(…) il Consiglio adotta una decisione che stabilisce le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale (…)*" (art. 39).
A partire dal 25 maggio 2018 vi è poi la piena applicabilità del Regolamento UE 2016/679 (GDPR) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e dall'agosto 2018 del nuovo Codice della Privacy[396] italiano.

---

390 In particolare, per quanto d'interesse viene tutelata la dignità umana (art. 1), il rispetto per la vita privata e familiare (art. 7), la protezione dei dati di carattere personale (art. 8), la non discriminazione (art. 21).
391 La Costituzione riconosce al lavoro un valore fondante del nostro ordinamento quando sancisce all'articolo 1 che l'Italia è una Repubblica democratica fondata sul lavoro. Le altre norme costituzionali che integrano il quadro dei principi si ritrovano negli articoli: 2 (diritti inviolabili della personal), 3 (uguaglianza formale e sostanziale), 4 (diritto al lavoro); 13 (diritti inviolabili della liberta personale); 35 (tutela il lavoro in tutte le sue forme ed applicazioni); art. 36 (riconosce alle donne «gli stessi diritti e, a parità di lavoro, le stesse retribuzioni che spettano al lavoratore»); art. 39 (garantisce e tutela l'organizzazione sindacale); art. 40 (garantisce il diritto di sciopero); art. 41,2 (limite al principio della libertà di iniziativa economica privata laddove ne vieta l'esercizio con modalità tali da pregiudicare la sicurezza e dignità umana).
392 I Principi Guida si articolano in tre differenti ambiti: 1) il dovere dello Stato di proteggere i diritti umani e le libertà fondamentali; 2) la responsabilità delle imprese di evitare un impatto negativo sui terzi e di rispettare i diritti umani; 3) la necessità per lo Stato di assicurare alle vittime dell'azione illecita delle imprese di ricorrere a rimedi adeguati ed effettivi.
http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf
393 https://cidu.esteri.it/resource/2016/12/49118_f_PANBHRITAFINALE15122016.pdf
394 Piano di Azione Nazione su Impresa e Diritti Umani, pag. 6.
395 Per un'analisi approfondita sul tema si rinvia al capitolo successivo.
396 D. Lgs. 196 del 30 giugno 2003 come modificato e integrato dal D. Lgs. 101 del 10 agosto 2018 recante "disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento UE 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonchè alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)".

I principali cambiamenti introdotti dal GDPR hanno riguardato: l'applicazione dei principi di "*data protection by design*" e di "*data protection by default*"[397] nei processi di sviluppo e lancio di nuove tecnologie, prodotti, servizi; l'obbligo di effettuare il *data protection impact assessment*[398] per i trattamenti che presentano rischi elevati e norme speciali sul trattamento con processi decisionali automatizzati e di profilazione[399]. Tutto ciò nell'ottica di una maggiore responsabilizzazione dei Titolari del trattamento al canone dell'*accountability*.
Da ultimo, con particolare riguardo al trattamento automatizzato di dati personali, la Convenzione di Strasburgo del 1981 (denominata Convenzione 108, da ultimo modificata nel 2018 per uniformarla al GDPR) costituisce lo strumento internazionale di tutela volto a garantire "*ad ogni persona fisica, quali che siano la sua nazionalità o la sua residenza, il rispetto dei suoi diritti e delle sue libertà fondamentali, e in particolare del suo diritto alla vita privata, in relazione all'elaborazione automatica dei dati a carattere personale che la riguardano («protezione dei dati»)*"[400].
La disciplina privacy è implementata da numerose pronunce interpretative fornite dalle Autorità di Controllo[401] *attive a livello nazionale e internazionale.*

L'utilizzo di tecniche di *Data Analyst* consente di elaborare anche i cosiddetti *Big Data* prodotti dalla digitalizzazione del lavoro.
Con il concetto di *Big Data* ci si riferisce, secondo quanto precisato dal Garante Europeo[402], alla raccolta, analisi e accumulo ricorrente di ingenti quantità di dati (anche personali) provenienti da fonti eterogenee e oggetto di un trattamento automatizzato mediante tecniche avanzate di analisi al fine di individuare correlazioni, tendenze e modelli.
Anche in materia di *Big Data* non esiste attualmente una normativa organica che ne disciplini l'uso, ma sono oggetto di raccomandazioni e linee guida elaborate dalle Istituzioni europee, in particolare dal Parlamento[403] e Consiglio[404].
I provvedimenti, oltre a contemplare le potenzialità connesse all'uso dei Big Data, ne descrivono le problematicità essendo in grado di *"condurre non solo a violazioni dei diritti fondamentali dei singoli, ma anche a disparità di trattamento e a una discriminazione indiretta nei confronti di gruppi di persone con caratteristiche simili, in particolare per quanto concerne l'equità e le pari opportunità di accesso all'istruzione e all'occupazione, quando si offre un lavoro alla persona o la si valuta*"[405].

397 Art. 25 GDPR.
398 Art. 35 GDPR.
399 Art. 22 GDPR.
400 Art. 1 Convenzione di Strasburgo.
401 A livello italiano il Garante per la Protezione dei Dati Personali (GPDP), a livello europeo il Garante Europeo (GEPD), l'*European Data Protection B*oard (ex WP29).
402 EDPS Opinion 7/2015 *Meeting the challenges of Big Data signora A call for transparency, user control, data protection by design and accountability* del 19.11.2015 https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf.
403 Si ricordano la Risoluzione del Parlamento europeo del 14 marzo 2017 sulle implicazioni dei *Big Data* per i diritti fondamentali: *privacy*, protezione dei dati, non discriminazione, sicurezza e attività di contrasto (2016/2225(INI)) e la comunicazione "*Una strategia europea per i dati*" della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni del 19.02.2020
404 Si cita la Raccomandazione CM/Rec(2010)13 del Comitato dei Ministri del Consiglio d'Europa agli Stati membri sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale nel contesto delle attività di posto a un'altezza inaccessibile
405 Punto 19 della Risoluzione del Parlamento europeo del 14 marzo 2017 sulle implicazioni dei Big Data per i diritti fondamentali: *privacy*, protezione dei dati, non discriminazione, sicurezza e attività di contrasto (2016/2225(INI)).

Perplessità che sono condivise anche dal Garante Europeo[406] e dall'European Data Protection Board (ex WP29)[407] e che hanno portato il Garante per la Protezione dei Dati Personali, congiuntamente con le Autorità di controllo AGCM e AGCOM, a promuovere un'indagine conoscitiva sui Big Data conclusasi il 10 febbraio 2020[408]. Da ultimo sul tema si cita la proposta di Regolamento Europeo denominato *Data Governance Act* (DGA)[409] che mira a disciplinare la disponibilità e l'utilizzo dei Big Data tra Pubbliche amministrazioni e soggetti privati, favorendone la circolazione e consentendo il trattamento mediante l'aiuto di un "intermediario per la condivisione dei dati personali".

Non possono, poi, essere trascurate le tematiche connesse all'Intelligenza Artificiale oggetto di recenti studi volti a delineare lo sviluppo dell'AI e alla redazione di una disciplina regolatrice.
Dopo la pubblicazione nel 2019 dello studio compiuto dal Parlamento Europeo[410] e delle Linee Guida della Commissione Europea[411] è, infatti, del 2020 la pubblicazione del *White Paper* della Commissione Europea sull'Intelligenza Artificiale in cui si evidenzia il rapido sviluppo dei sistemi di AI definiti un *"insieme di tecnologie che combina dati, algoritmi e potenza di calcolo*"[412]. Nel documento si identificano, inoltre, i progressi compiuti nell'ambito del calcolo e la crescente disponibilità di dati quali fattori determinanti del celere sviluppo dell'Intelligenza Artificiale.
L'evoluzione dell'IA, secondo la Commissione, comporterà miglioramenti nella vita di ognuno, ma al contempo può determinare "*una serie di rischi potenziali, quali meccanismi decisionali opachi, discriminazioni basate sul genere o di altro tipo, intrusioni nelle nostre vite private o utilizzi per scopi criminali*"[413].
Lo studio della Commissione ha portato il 21 aprile 2021 alla presentazione di una proposta di Regolamento sull'Intelligenza Artificiale ove, nell'ottica di uno sviluppo proporzionato della IA nel rispetto dei diritti fondamentali, promuove l'utilizzo di tali tecniche anche nel mondo di lavoro proponendo un approccio *risk based* e indicando tra i sistemi di IA ad alto rischio quelli impiegati per "*istruzione e formazione professionale*" nonché per "*occupazione, gestione dei lavoratori e accesso al lavoro autonomo*"[414].
La rilevanza e il rapido sviluppo dell'IA e la contestuale presenza di rischi potenziali a essa connessi è stata altresì contestualizzata dal Ministero per lo Sviluppo Economico italiano nel documento del 2 luglio 2020 denominato "Strategia italiana per l'Intelligenza Artificiale"[415].

---

406 Il Garante Europeo si è pronunciato sul tema dei Big Data nel parere 4/2015 *Towards a New Digital Ethics: data, dignity an technology*, settembre 2015; nel parere 7/2015 del 19 novembre 2015, dal titolo "*Meeting the challenges of Big Data – A call for transparency, user control, data protection by design and accountability"* e nel parere 8/2016 del 23 settembre 2016, intitolato "*EDPS Opinion on coherenta un'altezza di 6 o 7 metri of fundamental rights in the age of Big Data*".
407 EDPB *Preliminary Opinion of the European Data Protection Supervisor Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Econom,* marzo 2014.
408 Indagine conoscitiva sui *Big Data* condotta congiuntamente da Autorità Garante della Concorrenza e del Mercato (AGCM), Autorità per le Garanzie nelle Comunicazioni (AGCOM), e dal Garante per la Protezione dei Dati Personali (GPDP) del 10 febbraio 2020, visibile su sito del Garante la Protezione dei Dati Personali https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9264204.
409 Regolamento del Parlamento europeo e del Consiglio relativo alla *governance* europea dei dati" (c.d. *Data Governance Act*) presentato dalla Commissione il 25 novembre 2020 consultabile sul sito https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767. A riguardo Scagliarini S., *Identità digitale e tutela della privacy,* atti del Convegno annuale Associazione Gruppo di Pisa "*Il diritto costituzionale e le sfide dell'innovazione tecnologica",* Genova 18/19 giugno 2021, pp. 42 – 44.
410 Studio del Parlamento Europeo "*Opportunities che non apparteneva alla signora. Artificila Intelligence*" del giugno 2020.
411 https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.
412 Pag. 2 del White Paper della Commissione Europea sull'Intelligenza Artificiale.
413 Pag. 1 del White Paper della Commissione Europea sull'Intelligenza Artificiale.
414 Allegato III "*che il trattamento meno favorevole patito dalla signora Coleman, lavoratrice presso studio legale,*" punti 3 e 4.
415 Accessibile al sito https://www.mise.gov.it/images/stories/documenti/Proposte_per_una_Strategia_italiana_AI.pdf

Si deve, inoltre, fare riferimento alla Proposta della Commissione Europea di Direttiva[416] per il miglioramento delle condizioni di lavoro mediante piattaforma del 9 dicembre 2021.
La Proposta di Direttiva, riferendosi ai lavoratori che svolgono la propria attività mediante piattaforme digitali[417], enuncia alcuni principi rilevanti in riferimento alla gestione algoritmica.
Indicazioni che possono trovare applicazione analogica nei contesti lavorativi che, pur non essendo definibili "piattaforme", impiegano processi di *Data Drive Management* o di *Algoritmic Management*[418].
Tra i vari obiettivi che la Direttiva si prefigge d'introdurre vi è anche quello di garantire l'equità, la trasparenza e la responsabilità nella gestione algoritmica dei rapporti di lavoro (in merito gli artt. 6 – 10 della Direttiva).
In particolare, l'art. 6 dispone l'obbligo, a capo degli Stati membri, d'introdurre un diritto di informazione ai singoli lavoratori sia sui sistemi di controllo delle prestazioni lavorative, sia sui c.d. *automated decision making systems*, ossia i sistemi che assumono decisioni automatiche in relazione alle condizioni di lavoro (paragrafo 1).
Sempre l'art. 6, al paragrafo 5, ponendosi di garantire l'equità e la trasparenza del trattamento, dispone che le piattaforme di lavoro digitale non possano in alcun modo elaborare dati personali dei lavoratori se non strettamente connessi alla loro prestazione lavorativa. Il principio si colloca in linea con la tutela nazionale prevista dall'art. 8 SL.
Gli articoli 7 e 8 della Proposta di Direttiva analizzano specificatamente il monitoraggio e il riesame umano dei sistemi algoritmi e delle decisioni dagli stessi assunte.
In particolare, l'art. 7 *"impone alle piattaforme di lavoro digitali di monitorare e valutare periodicamente l'impatto sulle condizioni di lavoro delle decisioni individuali prese o sostenute da sistemi decisionali e di monitoraggio automatizzati*"[419].
Dovranno, quindi, essere valutati periodicamente i rischi dei sistemi decisionali e di monitoraggio automatizzati anche in riferimento alla salute e sicurezza dei lavoratori e garantire "*che tali sistemi non esercitino in alcun modo una pressione indebita sui lavoratori delle piattaforme digitali o mettano altrimenti a rischio la loro salute fisica e mentale*"[420].
Il terzo paragrafo del medesimo articolo stabilisce, inoltre, che i sistemi di monitoraggio automatizzati vengano a loro volta controllati da operatori umani al fine di proteggere i lavoratori da conseguenze

---

416 *Proposal for a Directive of the European Parliament and of the Council on improving working conditions in platform work, COM/2021/762* in *www.eur-lex.europa.eu*.
417 L'articolo 2 della Proposta di Direttiva definisce la "*piattaforma di lavoro digitale*" come "*qualsiasi persona fisica o giuridica che fornisce un servizio commerciale che soddisfa tutti i requisiti seguenti:*
a) è fornito, almeno in parte, a distanza con mezzi elettronici quali un sito web o un'applicazione mobile;
b) è fornito su richiesta di un destinatario del servizio;
c) comporta, quale componente necessaria ed essenziale, l'organizzazione del lavoro svolto dalle persone fisiche, indipendentemente dal fatto che tale lavoro sia svolto online o in un determinato luogo".
Lo stesso articolo definisce anche i concetti di:
"*lavoro mediante piattaforme digitali*" facendo riferimento a "*qualsiasi lavoro organizzato tramite una piattaforma di lavoro digitale e svolto nell'Unione da persone fisiche sulla base di un rapporto contrattuale tra la piattaforma di lavoro digitale e la persona fisica, indipendentemente dal fatto che esista o no un rapporto contrattuale tra tale persona e il destinatario del servizio*";
"persona che svolge un lavoro mediante piattaforme digitali", intendendo "*qualsiasi persona fisica che svolge un lavoro mediante piattaforme digitali, indipendentemente dalla qualificazione contrattuale, da parte delle parti interessate, del rapporto tra tale persona e la piattaforma di lavoro digitale*";
"*lavoratore delle piattaforme digitali*" indicando "*qualsiasi persona che svolge un lavoro mediante piattaforme digitali e ha un contratto di lavoro o un rapporto di lavoro quali definiti dal diritto, dai contratti collettivi o dalle prassi in vigore negli Stati membri, tenuto conto della giurisprudenza della Corte di giustizia*".
418 Cfr. Lo Faro A., *Algorithmic Decision Making e gestione dei rapporti di lavoro: cosa abbiamo imparato dalle piattaforme*, in *Federalismi.it* del 5 ottobre 2022, n. 25, pp. 189 ss.
419 Proposta di Direttiva pag. 18.
420 Elaborare dati al fine d'interpretarli e individuare eventuali correlazioni, impiegando tecniche di analisi avanzate, incrementa le Proposta di Direttiva pag. 18.

negative integramente automatizzate, quali licenziamenti, altre sanzioni disciplinari o trattamenti sfavorevoli.
L'articolo 8 riconosce, contestualmente, il diritto in capo al lavoratore di chiedere spiegazioni alla piattaforma in merito a una determinata decisione che abbia significativamente leso le sue condizioni lavorative (come può essere la sospensione o la chiusura dell'*account*).
L'articolo al secondo paragrafo disciplina, inoltre, il diritto di reclamo del lavoratore.
La Proposta di Direttiva rimarca, infine, l'importanza della trasparenza delle logiche poste a fondamento dei sistemi algoritmici, introducendo ulteriori tutele con gli articoli 11 e 12.
In particolare, l'art. 12 richiede alle piattaforme di rendere semestralmente accessibili determinate informazioni, sia alle autorità pubbliche vigilanti sul lavoro, sia alle rappresentanze sindacali dei lavoratori su piattaforma. Tali informazioni riguardano, a titolo esemplificativo, il numero di persone che lavorano su piattaforma, la qualificazione giuridica del loro rapporto nonché le condizioni contrattuali loro applicabili in virtù della qualificazione medesima.
Le tutele previste dalla Proposta di Direttiva risultano, quindi, orientate a garantire nuovi e più specifici diritti ai lavoratori soggetti a un *Algorithmic Management,* cercando di rendere comprensibile le logiche con cui i compiti possono venire assegnati dalla piattaforma e nonché rendendo trasparenti (ove possibile) le aree d'intervento dei sistemi automatici nell'organizzazione del lavoro.

Nell'utilizzare strumenti di *Data Analyst* applicati all'analisi dei lavoratori non ci si può esimere dal richiamare le tutele giuslavoristiche nazionali e, in particolare, lo Statuto dei Lavoratori (con riguardo agli articoli 4 e 8 analizzati in precedenza e alla disciplina *privacy*[421] richiamata dalla norma sui controlli a distanza) e le norme sulla discriminazione diretta e indiretta previste dai D. Lgs. 215 e 216 del 2003.
Il diritto antidiscriminatorio trova, inoltre, espressione in un insieme di principi e disposizioni di legge dell'UE che tutelano le persone dai pregiudizi basati su sesso, razza, origine etnica, disabilità, religione, età e orientamento sessuale.
Le tutele che interessano specificatamente i lavoratori si estrinsecano nella Direttiva 2006/54/CE (in riferimento alla differenza di genere), nella Direttiva 2000/43/CE (inerente alle disuguaglianze per motivi di razza o origine etnica) e nella Direttiva 2000/78/CE (sulle discriminazioni attuate in base a disabilità, religione o convinzioni personali, età e orientamento sessuale). Il principio generale di non discriminazione nel diritto dell'UE abbraccia, così, il mercato del lavoro secondo un'ampia prospettiva di tutela.

La Proposta di Direttiva è stata oggetto di emendamenti da parte del Parlamento Europeo, Commissione per l'Occupazione e gli Affari Sociali, con modifiche introdotte il 21 dicembre 2022 (A9-0301/2022).
Le novità proposte dal Parlamento Europeo affrontano il tema della tutela collettiva[422] dei lavoratori su piattaforma, ampliando la definizione dei soggetti che possono intervenire in qualità dei rappresentanti dei lavoratori e allargando le prerogative agli stessi attribuite.

---

421 Forte è, infatti, il rinvio formulato al comma 3 dallo stesso art. 4 dello St. dei Lavoratori il quale recita: "*le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196"* (art. 4 comma 3 Statuto dei Lavoratori). Cfr. Ingrao A., *Il controllo a distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata*, Cacucci Editore, Bari, 2018.

422 Il nuovo Considerando 18bis promuove la creazione di sindacati più rappresentativi e che le elezioni per i rappresentanti dei lavoratori rispettino i diritti e le libertà fondamentali. Al nuovo Considerando 18ter si legge poi che "*Il dialogo sociale e la contrattazione collettiva rivestono la massima importanza ai fini del raggiungimento degli obiettivi della presente direttiva. È opportuno preservare le prerogative esclusive dei sindacati, come il loro diritto di partecipare alla contrattazione collettiva e di concludere contratti collettivi. I diritti e le prerogative dei sindacati e degli altri rappresentanti dei lavoratori di cui alla presente direttiva dovrebbero essere garantiti e rispettati in linea con le convenzioni dell'ILO e con la Carta sociale europea del Consiglio d'Europa"*. Parimenti al Considerando 23 come emendato si legge che

Ciò al fine di garantire un maggior coinvolgimento dei rappresentanti dei lavoratori non solo per salvaguardare diritti individuali, ma anche collettivi azionabili mediante un'azione diretta.
Espressione di tale finalità si ritrova, per esempio, nell'art. 6 paragrafo 1 comma 1[423], come emendato, il quale riconosce un diritto di informazione collettivo ravvisando i rappresentanti dei lavoratori (e non i singoli prestatori) quali primi destinatari delle informazioni sull'esistenza e sul funzionamento dei sistemi automatizzati di controllo e decisionali.
Parimenti, all'art. 8 paragrafo 2 comma 1 viene riconosciuto ai lavoratori delle piattaforme digitali e ai loro rappresentanti il diritto di chiedere alla piattaforma il riesame delle decisioni adottate mediante un sistema automatizzato.
La trasparenza del trattamento passa, quindi, mediante un diritto di informazione che è destinato non più solo ai singoli, ma coinvolge *in primis* i rappresentanti.

Gli interventi del Parlamento Europeo si orientano, inoltre, verso un rafforzamento della trasparenza del trattamento prevedendo che vengano ampliate le informazioni che devono essere comunicate ai lavoratori e ai loro rappresentanti (Considerando 32[424] emendato).
Le modifiche apportate prevedono, per esempio, che vengano rese note le categorie di dati monitorati, supervisionati o valutati dal sistema[425], le modalità con cui il sistema deve conseguire l'obiettivo del monitoraggio[426] e che sia condiviso il documento di valutazione di impatto predisposto ai sensi dell'art. 35 del GDPR[427].
Il Parlamento Europeo ha, infatti, imposto l'obbligo alle piattaforme digitali di coinvolgere i rappresentanti nel compimento degli adempimenti previsti per redigere una valutazione di impatto del trattamento dei dati. La piattaforma è, quindi, tenuta a raccogliere il parere dei rappresentanti dei lavoratori sul trattamento previsto (articolo 6, paragrafo 5 bis), coinvolgerli nella valutazione (articolo 7, paragrafo 1) e presentare il documento finale compilato (articolo 7, paragrafo 2bis).
Il rafforzamento del diritto di informazione, secondo una dimensione collettiva, risulta finalizzato a consentire un intervento effettivo dei lavoratori e dei loro rappresentanti, permettendo di attivare strumenti collettivi di tutela quali la contrattazione[428] o la consultazione.
L'invito a ricorrere alla consultazione collettiva viene ben evidenziato dal nuovo paragrafo 2bis dell'art. 9 ove si legge che "*le piattaforme di lavoro digitali forniscono ai rappresentanti dei lavoratori le informazioni di cui all'articolo 6, paragrafi 1, 2, 5 bis e 5 ter, e all'articolo 7 in tempo utile per consentire un esame approfondito e una consultazione efficace (…)*"[429].

"(…) *La contrattazione collettiva è uno strumento fondamentale con cui migliorare le condizioni* di lavoro *delle persone che svolgono un lavoro mediante piattaforme digitali, indipendentemente dalla designazione contrattuale del rapporto*, *e dovrebbe essere incoraggiata dalla Commissione e dagli Stati membri".*

423 Emendamento 113 del Parlamento europeo "*Fatti salvi gli obblighi e i diritti delle piattaforme di lavoro digitali e dei lavoratori delle piattaforme digitali a norma del regolamento (UE) 2016/679 e delle direttive 89/391/CEE, 2009/38/CE e (UE) 2019/1152, gli Stati membri impongono alle piattaforme di lavoro digitali di informare i lavoratori delle piattaforme digitali, i rappresentanti dei lavoratori e gli ispettorati del lavoro e le autorità competenti (…)"*

424 Nell'emendamento 42 del Parlamento europeo si legge "(…) *I singoli lavoratori delle piattaforme digitali dovrebbero ricevere tali informazioni in forma concisa, semplice e comprensibile, nella misura in cui i sistemi e le loro caratteristiche incidono direttamente su di loro e sulle loro condizioni di lavoro, in modo da essere effettivamente informati. Poiché sono necessarie informazioni più dettagliate ai fini della piena trasparenza, della consultazione e della negoziazione efficaci tra le parti e dell'applicazione delle norme, le piattaforme di lavoro digitali dovrebbero anche fornire una relazione dettagliata e solida contenente tali informazioni per i lavoratori delle piattaforme digitali, i loro rappresentanti e le autorità competenti".*

425 Art. 6, paragrafo 2, lettera a, punto IIe lettera b, punto III.

426 Art. 6, paragrafo 2, lettera a, punto ii bis (nuovo).

427 Si vedano i nuovi Considerando 32ter, Considerando 38bis, Art. 6, paragrafo 5 bis, Art. 7, paragrafo 1, Art. 7, paragrafo 2 bis

428 In nuovo art. 10bis prevede espressamente la *Promozione della contrattazione collettiva nel lavoro mediante piattaforme digitali.*

429 La norma prosegue prevedendo che "*Per i sistemi automatizzati di nuova introduzione, la consultazione ha luogo prima del loro utilizzo e prima di qualsiasi modifica che incida sulle condizioni di lavoro, sull'organizzazione del lavoro o sul monitoraggio dell'esecuzione del lavoro".*

Informazioni che devono essere fornite direttamente dalla piattaforma o dal fornitore di servizi.
La novella prevede, dunque, che i rappresentanti dei lavoratori siano posti nella condizione di comprendere il trattamento e gli effetti che questo produce, affinché il loro intervento sia valido e concreto.
A tal fine, gli emendamenti introdotti dal Parlamento Europeo sottolineano come le informazioni fornite ai lavoratori o ai loro rappresentanti (incluse le decisioni assunte dalla piattaforma) devono essere condivise in modo "*trasparente e intelligibile, utilizzando un linguaggio semplice e chiaro*"[430] e che queste devono essere comunicate in un tempo "utile" per azionare le tutele.
Il Parlamento Europeo intende, così, promuovere la cooperazione tra le parti mediante l'introduzione di previsioni che consentano un coinvolgimento effettivo e una partecipazione attiva degli interessati (o dei loro rappresentanti) nel processo di valutazione e progettazione del trattamento automatizzato.

[430] Art. 8 commi 1 e 2; Art. 9, paragrafo 1.

Capitolo 4
Trattamenti automatizzati e privacy dei lavoratori

1. La tutela dei dati personali. I sistemi decisionali automatizzati e la profilazione

La digitalizzazione del luogo di lavoro, con l'implementazione di applicazioni sempre più autonome, abilita la comprensione di nuove informazioni mediante la correlazione e l'elaborazione di dati.
In riferimento a tali novità, nei capitoli precedenti si è avuto modo di riscontrare alcune problematiche, intrinsecamente connesse alla natura dei dati acquisiti e alle fallaci valutazioni che possono essere compiute *ex ante* all'utilizzo dei medesimi.
Ove i dati siano caratterizzati da una "non evidenza" e si renda necessaria una fase interpretativa, le riflessioni coinvolgono inevitabilmente l'utilizzabilità degli stessi e le tutele poste a presidio della riservatezza dei lavoratori.
Appare, quindi, necessaria una riflessione sui tipi di trattamenti che possono essere compiuti con particolare riguardo a quelli caratterizzati da un elevato o totale grado di autonomia.
Ci si domanda, infatti, se sussista un bilanciamento tra i rinnovati interessi datoriali, in grado di accedere ad un numero crescente di informazioni e di avvalersi di strumenti automatizzati, e il diritto dei lavoratori a tutelare i dati personali.

Il diritto alla protezione dei dati personali viene riconosciuto a livello europeo a partire dagli anni Novanta, a seguito dell'emanazione della "Direttiva madre" del 1995 (Direttiva 95/45/CE) e dell'art. 8 della Carta di Nizza.
In Italia la tutela dei dati personali ha trovato, però, un'iniziale fondamento ben prima delle previsioni europee già all'interno della disciplina statutaria. L'art. 8 dello Statuto dei Lavoratori sancisce, infatti, il divieto intangibile per il datore di lavoro di compiere indagini sulle opinioni politiche, religiosi i sindacali del lavoratore.
La norma riconosce, quindi, alle informazioni attinenti alla vita di un lavoratore una protezione ultronea rispetto a quella "generica" posta a tutela dello spazio psico-fisico individuale che deve essere preservato da indebite intrusioni.
Lo Statuto dei Lavoratori tutelando la "libertà" e la "dignità" del lavoratore interpreta, così, la doppia dimensione giuridica della protezione dei dati personali garantendo la libertà "negativa" di un prestatore a non essere illecitamente sorvegliato, ma anche quella "positiva" assicurando un controllo attivo sui dati acquisiti.

Con l'emanazione della Direttiva 95/45/CE e del D. Lgs 196/2003, di attuazione a livello nazionale, la disciplina sulla riservatezza dei dati personali nell'ambito del rapporto di lavoro ha previsto l'applicazione di specifici trattamenti al fine di garantire tutele rafforzate e limitazioni ulteriori rispetto al regime normativo generale.
Tale previsione rispecchia il peculiare rapporto "asimmetrico" instaurato tra lavoratori (esecutori del contratto di lavoro e interessati al trattamento dei dati) e datori di lavoro (Titolari dei dati personali acquisiti in forza del rapporto in essere).
Anche il Regolamento Generale Europeo sulla Protezione dei Dati Personali (Regolamento UE 2016/679 – GDPR), pur emanando una disciplina direttamente applicabile, recede dinanzi alle specificità normative giuslavoristiche e sindacali dei singoli stati membri.

L'art. 88[431] del GDPR stabilisce, infatti, che i singoli Stati possano prevedere, attraverso una normazione di rango primario, regole più specifiche per assicurare la tutela dei diritti e delle libertà dei prestatori in relazione al trattamento dei loro dati personali acquisiti in ragione del rapporto di lavoro.
La norma delinea, quindi, un delicato bilanciamento tra interessi datoriali e tutele riconosciute ai dipendenti cercando di integrare e conformare le norme giuslavoristiche nazionali con i principi europei.
Obiettivo sicuramente complesso che, a livello nazionale, è supportato dall'intervento ricognitivo e interpretativo del Garante per la Protezione dei Dati Personali (GPDP) che attraverso strumenti di "*soft law*" pondera i distinti trattamenti compiuti nell'ambito dei rapporti di lavoro, valutando finalità, modalità di trattamento e misure di sicurezza.
Intervento che è stato sancito anche dal Legislatore nazionale nell'art. 11 del Codice in materia di protezione dei dati personali (così come novellato dal D. Lgs 101/2018), prevedendo che il GPDP possa adottare regole deontologiche per i soggetti pubblici e privati che compiono trattamenti dei dati personali nell'ambito dei rapporti di lavoro.

Il trattamento dei dati personali nel contesto lavorativo è, inoltre, caratterizzato dell'utilizzo di dispositivi digitali che, in maniera sempre crescente, coadiuvano i lavoratori nell'esecuzione delle prestazioni.
Tecnologia che, come si è avuto modo di illustrare nei capitoli precedenti, espone i lavoratori a un possibile controllo capzioso e minuzioso, in particolar modo quando la sorveglianza interessi dati "non autoevidenti" il cui significato diviene intellegibile solo a seguito di un'elaborazione interpretativa.
Le potenzialità di analisi dei sistemi algoritmici e di IA permettono, infatti, d'individuare modelli di correlazione in grado di definire aspetti che non sono inerenti ad ambiti professionali e che concernono aspetti personali.
I "lavoratori digitali" possono, quindi, trovarsi oggetto di trattamenti decisionali automatizzati o di profilazione, ai sensi dell'art. 22 del GDPR, in ragione del processo interpretativo compiuto.
Profili e decisioni che possono strutturarsi non solo su accurate osservazioni dell'attività lavorativa svolta, ma anche su elementi attinenti alla sfera intima degli interessati.
Il datore di lavoro può, così, venire a conoscenza di informazioni relative le convinzioni personali che potrebbero non corrispondere alle reali caratteristiche identitarie del prestatore.
Anche quando l'analisi algoritmica interessi elementi pertinenti al rapporto di lavoro possono comunque generarsi alterazioni nella definizione dell'identità professionale del singolo.

L'impiego di queste tecnologie può, quindi, incidere contestualmente sull'esercizio del potere di controllo datoriale, incrementandolo, e sulla tutela dei dati personali, indebolendola.
La centralità definitoria del "controllo a distanza" a seguito dell'evoluzione digitale ha visto, quindi, chiamare direttamente in causa la normativa *privacy* che, con l'emanazione del D. Lgs. 151/2015 intervenuto sul testo dell'art. 4 SL, ha delineato i limiti dell'utilizzabilità dei dati.

1.1. I principi generali

La ricerca di un bilanciamento tra le nuove potenzialità acquisite dai poteri datoriali e il diritto alla *privacy* dei lavoratori parte dallo studio dei testi normativi, primo fra tutti il Regolamento UE 2016/679

[431] Art 88 GDPR "*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*".

(Regolamento Generale sulla Protezione dei Dati o GDPR), che all'articolo 5 enuncia i principi applicabili ad ogni trattamento dei dati personali.
La norma prevede che il trattamento debba rispettare i criteri di:

- liceità, correttezza e trasparenza.
- finalità;
- minimizzazione;
- esattezza;
- conservazione;
- integrità;
- responsabilizzazione.

Tali principi, validi universalmente, devono essere tenuti in particolare riguardo per i trattamenti posti in essere con tecnologie abilitanti nei confronti di soggetti vulnerabili[432] quali sono i lavoratori.
I dati dei lavoratori devono, quindi, essere trattati in modo lecito, equo e trasparente (principio di liceità, equità e trasparenza).
I medesimi devono essere raccolti per uno scopo specifico, esplicito e legittimo e non devono essere sottoposti a trattamenti ulteriori e incompatibili alla finalità indicata (principio di finalità).
I dati dei lavoratori utilizzati devono essere adeguati, pertinenti e non eccedenti rispetto alle finalità che ne giustificano il trattamento (principio di minimizzazione).
I dati devono essere esatti e aggiornati tempestivamente ove necessario. Il datore di lavoro deve, quindi, prendere tutte le misure ragionevoli per rettificare o cancellare i dati non corretti rispetto alle finalità perseguite e dichiarate (principio di esattezza).
I dati devono essere integri, ovvero accurati. Il datore di lavoro ha, quindi, l'onere di garantire la cancellazione o la correzione di dati incompleti, avendo riguardo alle finalità per le quali essi sono stati raccolti[433] (principi di integrità).
Il datore di lavoro è, inoltre, chiamato a dar prova che il trattamento sia avvenuto in modo conforme alla normativa *privacy* nonché di avere adottato tutte le misure necessarie a ridurre i rischi legati all'utilizzo dei dati acquisiti (principio di responsabilizzazione o di *accountability*).
Ulteriori principi generali di rilievo sono il principio di proporzionalità e trasparenza.
La trasparenza impone che le informazioni destinate al lavoratore siano accessibili, di facile comprensione e che, nel fornirle, sia impiegato un linguaggio semplice e chiaro.
I lavoratori devono, quindi, essere informati preventivamente e concretamente sulla tipologia di dati raccolti e sulle finalità delle operazioni di trattamento previste o effettuate.
Sussiste, infine, l'obbligo di garantire la proporzionalità del trattamento rispetto ai rischi che il lavoratore può subire in ragione del trattamento medesimo. Di conseguenza, ogni attività che comporti l'osservabilità e, dunque, il potenziale controllo dei lavoratori deve costituire una "*risposta proporzionata del datore di lavoro ai rischi che si trova ad affrontare, tenendo conto del legittimo interesse dei lavoratori alla privacy e di altri interessi*"[434].

---

[432] Questo è quanto emerge da quanto espresso dal Gruppo di lavoro ex Articolo 29 nel parere WP258 secondo cui la condizione di disparità contrattuale tra le parti del rapporto lavorale può porre in una condizione di "assoggettamento" il lavoratore. Circostanza che, non permettete di accertare a priori la validità del consenso eventualmente prestato, inficiandone la validità.
[433] Cfr. GPDP https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1390186.
[434] Articolo 29 nel parere WP258 consultabile su https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1390186.

1.2. Le norme specifiche per i trattamenti automatizzati o di profilazione

Grazie all'ausilio di sistemi algoritmici o di IA, i dati dei lavoratori sono soggetti a trattamenti caratterizzati da un grado di autonomia crescente.

Prendendo in considerazione le operazioni volte a rendere intellegibili dati "non autoevidenti", ove queste siano compiute in maniera automatizzata e incidano significatamene sui diritti dei lavoratori ricadono nella tutela prevista dall'art. 22 del GDPR.

Il tema del trattamento completamente automatizzato di dati non è nuovo nella disciplina *privacy* e veniva affrontato già dalla Direttiva 95/46/CE che, all'art. 15, prevedeva il diritto degli interessati a non essere soggetti a decisioni basate unicamente su trattamenti automatizzati[435], salvo casi eccezionali.

In linea con quanto disposto dall'art. 15 della Direttiva, l'art. 22 del GDPR esordisce prevedendo quale regola generale il divieto di adottare una decisione basata esclusivamente su trattamenti automatizzati disponendo 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*" (art. 22 par. 1).

Il Regolamento, tuttavia, a differenza della Direttiva incorpora espressamente il peculiare trattamento di "profilazione" nell'assunto della norma.

Si deve tenere presente che le decisioni automatizzate e la profilazione non sono fattispecie identiche, ma categorie autonome che possono conseguentemente operare in modo indipendente, anche se spesso strettamente correlate tra loro[436].

Il GDPR definisce, infatti, la profilazione come " *qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali 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*" (art. 4, comma 1, n. 4).

Per decisioni automatizzate si intende, invece, il risultato di un processo decisionale svolto esclusivamente mediante mezzi tecnologici, ovvero senza alcun intervento umano.

L'ambito definitorio delle decisioni automatizzate è, pertanto, distinto rispetto a quello della profilazione, potendo essere assunte decisioni automatizzate senza che vi sia profilazione. Parimenti può essere attuato un trattamento di profilazione senza l'ausilio di mezzi tecnologici, ma esclusivamente con intervento umano.

Occorre precisare che il divieto sancito dall'art. 22 GDPR vale non per ogni trattamento automatizzato, ma solo per quelli capaci di produrre effetti giuridici sui diritti dell'interessato o incida significativamente sulla sua persona.

---

[435] Raccomandazione (2010)13 sulla protezione delle persone fisiche rispetto al trattamento automatizzato dei dati personali nell'ambito della creazione di profili del Comitato dei Ministri del Consiglio d'Europa.

[436] Linee guida in materia di decisioni automatizzate individualizzate e profilazione ai fini del Regolamento 2016/679*,* del Gruppo di lavoro sulla protezione dei dati dell'articolo 29, adottato il 3 ottobre, 2017 e rivisto il 6 febbraio 2018 (WP215rev.01), p. 8-9.

Il Gruppo di lavoro sulla protezione dei dati di cui all'articolo 29, nelle Linee guida approvate al riguardo, si occupa della distinzione tra le due categorie, cercando di chiarire allo stesso tempo i punti di separazione e contatto tra di loro: "*Le decisioni automatizzate hanno una portata diversa e possono parzialmente sovrapporsi o derivare dalla profilazione. Le decisioni basate esclusivamente sul trattamento automatizzato rappresentano la capacità di prendere decisioni con mezzi tecnologici senza il coinvolgimento umano. (...) Le decisioni automatizzate possono essere effettuate con o senza profilazione; la profilazione può avvenire senza prendere decisioni automatizzate. Tuttavia, entrambi non sono necessariamente attività indipendenti. Qualcosa che inizia come un semplice processo decisionale automatizzato può evolversi in un processo basato sulla profilazione, a seconda di come vengono utilizzati i dati. (...) Le decisioni che non si basano esclusivamente sul trattamento automatizzato possono comprendere anche la profilazione*".

Solo l'utilizzo delle informazioni derivati dal trattamento automatizzato e impiegate per assumere una decisione di tale natura è soggetto al divieto sancito dall'art. 22 GDPR.
Il primo elemento richiesto dal Regolamento per l'operatività della norma è che la decisione derivante da tale trattamento sia completamente automatizzata.
Il Legislatore europeo presta, così, particolare attenzione alle decisioni completamente automatizzate avvertendo i rischi peculiari che tale trattamento può comportare agli interessati[437].
Appare, pertanto, fondamentale comprendere cosa sia una "decisione completamente automatizzata" e quale sia il grado minimo di partecipazione umana per escludere l'ipotesi.
La questione non risulta di poco conto, dato che le decisioni assunte dalle organizzazioni appaiono quasi sempre supportate da un sistema informatico la cui efficienza può rilegare l'intervento umano su un piano marginale.
Sulla questione si è pronunciato il Gruppo di lavoro art. 29[438] (WP29) il quale ha sottolineato come debba ritenersi completamente automatizzata la decisione in cui l'azione umana sia ricondotta a un mero intervento simbolico. Solo una partecipazione significativa, con una reale influenza della persona nel processo decisionale, esime dal caratterizzare come autonomo un trattamento.
Ciò comporta una valutazione sulla "significatività" dell'intervento umano vagliando, per esempio, la frequenza con cui il Titolare del trattamento si adegui a quanto proposto dal sistema algoritmico oppure se ne discosti.
Ove l'intervento umano si limiti ad una mera operazione di supervisione o di approvazione del processo compiuto, la decisione elaborata dall'algoritmo o dal sistema di IA non può che essere definita come "completamente automatizzata" e rientrare nell'ambito dell'art. 22 GDPR.
Ulteriore elemento che aiutano comprendere se una decisione possa essere definita come "completamente automatizzata" è il grado di complessità dell'operazione a cui la decisione è sottoposta, tenendo conto del volume di dati trattati e la rapidità con cui la stessa è stata assunta.

I divieti sanciti all'utilizzo di trattamenti automatizzati trovano, però, alcune eccezioni elencate dallo stesso art. 22 del GDPR.
La norma citata al comma 2[439] lettera a) prevede che le decisioni automatizzate e la profilazione siano consentite se "*necessarie per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento*".
È facile notare come il contratto di lavoro rientri nella deroga quando tale tipologia di trattamenti sia necessaria per la conclusione o l'esecuzione del contratto.
Le decisioni completamente automatizzate e la profilazione sarebbero quindi legittime nell'ambito del rapporto lavorale in forza del sotteso rapporto contrattuale (o precontrattuale) e il Titolare sia in grado di dimostrare la necessità di compiere[440].

---

437 Riflessioni in merito ai rischi di decisioni assunte integralmente da sistemi automatizzati erano già stati espressi dalla Commissione delle Comunità europee nel documento COM (92) 422 def. – SYN 287, Bruxelles, del 15 ottobre 1992 contenente la proposta modificata di Direttiva dal Consiglio relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione dei dati in preparazione alla Direttiva 95/46. Alle pagine 27 e 28 vengono analizzate le decisioni automatizzate relative alle persone.

438 WP29 Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679 adottate il 3 ottobre 2017 ed emendate in data 6 febbraio 2018, pp. 23 ss.

439 Le altre ipotesi di deroga sono elencate alle lettere b) e c) del medesimo comma e ammettono tali trattamenti ove autorizzati dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato (lett. b) oppure si basino sul consenso esplicito dell'interessato lett. c).

440 WP29 Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679 adottate il 3 ottobre 2017 ed emendate in data 6 febbraio 2018, p. 26. In merito il WP29 nel documento fornisce il seguente esempio. "*Un'azienda pubblicizza un posto di lavoro vacante. Essendo il posto molto ambito, l'azienda riceve decine di migliaia di candidature. In ragione del volume eccezionalmente elevato di candidature l'azienda potrebbe ritenere che non sia possibile individuare i*

In ogni caso, il paragrafo 4 dell'art. 22 del GDPR dispone che, qualora le decisioni automatizzate siano consentite, non possano basarsi su categorie di dati particolari (ex art. 9 del GDPR), salvo che l'interessato abbia prestato il proprio consenso o il trattamento sia necessario per motivi di interesse pubblico sulla base di un diritto dell'Unione Europea o degli Stati membri.
Ipotesi che, nei rapporti di lavoro, risultano escluse.

La possibilità di compiere un trattamento completamente automatizzato o di profilazione in ambito lavorativo non legittima, però, la creazione di profili in maniera indiscriminata e il trattamento dovrà essere compiuto nel rispetto di condizioni che garantiscono la tutela dei lavoratori.
In primo luogo, dovrà essere rispettata la disciplina generale prevista dal GDPR per tutti i tipi di trattamento.
Dall'ottemperanza dei principi elencati dall'art. 5 del GDPR, con particolare riguardo alla trasparenza, derivano alcuni diritti degli interessati quali il diritto di informazione (art. 13 comma 2 lett. f) e 14 comma 2 lett. g) del GDPR) e il diritto di accesso (art. 15 comma 1 lett. h) del GDPR).
In riferimento al diritto di informazione il Regolamento prevede che il Titolare del trattamento informi l'interessato circa "*l'esistenza di decisioni automatizzate, compresa la profilazione, di cui all'articolo 22 commi 1 e 4*" e, almeno in tali casi, dovranno essere fornite "*informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato*".
Da tale assunto derivano una serie di doveri di trasparenza relativi all'obbligo di informare l'interessato sull'esistenza di decisioni automatizzate, la logica applicata al trattamento nonché in riferimento all'importanza e alle conseguenze previste da tali operazioni.
Per quanto riguarda l'esistenza delle decisioni automatizzate, la norma prevede che ogni interessato ne venga a conoscenza ove sottoposto a un trattamento di cui all'art. 22 del GDPR.
L'articolo riflette, quindi, il principio di limitazione delle finalità del trattamento - sancito dall'articolo 5 comma 1 lett. b) del GDPR - in forza del quale la finalità deve essere determinata ed esplicita.
Il Regolamento impone, però, non solo che sia comunicata l'esistenza di un trattamento automatizzato, ma che vengano segnalate anche le caratteristiche specifiche di tale operazione, rendendo intellegibile la logica sottesa all'elaborazione.
Tali informazioni devono essere sufficienti affinché l'interessato possa comprendere come il sistema operi ed elabori decisioni in base ai dati acquisiti.
Il datore di lavoro è tenuto, quindi, a garantire il diritto alla spiegazione delle decisioni assunte dal sistema algoritmico o di IA (Considerando n. 71 del GDPR) fornendo informazioni significative sulla logica utilizzata e sulle conseguenze che il trattamento può implicare.
Il contenuto di tale diritto risulta, però, complesso.
In primo luogo, perché non è definita la portata delle informazioni che devono essere comunicate al fine di garantire un'effettiva spiegazione sulla logica adottata da un sistema.
In secondo luogo, perché tale diritto di informazione può scontrarsi con altri diritti connessi all'impiego di strumenti tecnologici come il segreto industriale o la proprietà intellettuale.
Aspetto rilevato anche dal Regolamento nel Considerando n. 63 ove si legge che il diritto a ricevere una spiegazione non dovrebbe ledere "*i diritti e le libertà altrui, compreso il segreto industriale e aziendale e la proprietà intellettuale, segnatamente i diritti d'autore che tutelano il software*".

candidati idonei senza prima utilizzare mezzi unicamente automatizzati per scartare le candidature non pertinenti. In questo caso potrebbe essere necessario ricorrere a un processo decisionale automatizzato per stilare un elenco ristretto di possibili candidati allo scopo di stipulare un contratto con un interessato".

Una totale trasparenza in merito alla logica delle decisioni assunte può, inoltre, risultare limitata o parziale nel caso (diffuso) in cui il datore di lavoro ignori come lo strumento automatizzato operi concretamente per via dell'alta complessità tecnica sottesa al funzionamento.
In merito alla logica utilizzata il Gruppo di lavoro art. 29 per la protezione dei dati, 3 ottobre 2017 (modificato il 6 febbraio 2018, 28) ha chiarito che "*il Titolare del trattamento dovrebbe trovare modi semplici per comunicare all'interessato la logica o i criteri sui quali si basa l'adozione della decisione. Il regolamento impone al titolare del trattamento di fornire informazioni significative sulla logica utilizzata, ma non necessariamente una spiegazione complessa degli algoritmi utilizzati o la divulgazione dell'algoritmo completo. Le informazioni fornite dovrebbero tuttavia essere sufficientemente complete affinché l'interessato possa comprendere i motivi alla base della decisione*".
Non risulta, dunque, necessario che venga spiegato il funzionamento dell'algoritmo sotteso al trattamento automatizzato, ma dovranno essere rappresentati i criteri in base ai quali le decisioni vengono prese e l'interessato possa comprendere i motivi posti alla base delle medesime.
L'importanza del principio[441] di conoscibilità del processo automatizzato e di comprensibilità delle conseguenze che tale trattamento può addurre dovrebbe, quindi, portare a condividere informazioni significative, inclusi i casi di studio impiegati per addestrare il sistema algoritmico.
Tra le prime informazioni che devono essere fornite vi è l'indicazione di quali dati o categorie di dati sono stati utilizzati per il *training*[442], nonché il distinto grado di rilevanza che a questi è attribuito così da intendere le ragioni delle distinte ponderazioni.
Risulta, inoltre, necessario comunicare i modelli relativi alla logica stimata, ovvero agli *output*, che presumibilmente si possono ottenere dagli *input* inseriti.
Ad esempio, se l'*input* è costituito dai dati "non autoevidenti" dei lavoratori, inizialmente anche non personali, l'*output* potrebbe interessare informazioni personali come le opinioni del lavoratore.
Al fine di favorire una maggior comprensione della logica applicata e delle conseguenze attese dal trattamento, il GDPR definisce le modalità con cui le informazioni devono essere comunicate prevedendo che queste siano redatte in forma concisa, trasparente, intellegibile, facilmente accessibile e siano espresse in un linguaggio semplice e chiaro (art. 12 comma 1 GDPR).
Le informazioni devono, quindi, essere flessibili, non eccessivamente tecniche e funzionali, risultando utili all'interessato per comprendere il trattamento automatizzato e ad azionare il diritto di opposizione.

L'articolo 15 comma 1 lett. h), in termini del tutto analoghi a quanto previsto dagli articoli 13 comma 2 lett. f) e 14 comma 2 lettera g), autorizza l'interessato ad esercitare il diritto di accesso anche in relazione al trattamento automatizzato di cui all'articolo 22 comma 1 del GDPR.
In tal modo il Legislatore europeo ha previsto non solo che l'interessato venga informato del trattamento prima che siano acquisiti i dati personali, ma che questi possa conoscere in ogni momento la logica e le conseguenze derivanti dal trattamento medesimo.

Oltre a tali previsioni generiche, il Titolare del trattamento deve adottare misure specifiche volte a garantire la trasparenza del trattamento e l'intervento umano per il riesame della decisione (ex art. 22 par. 3 GDPR).

---

[441] In ambito di decisioni amministrative automatizzate il principio è stato riconosciuto dalla giurisprudenza nelle pronunce del Cons. di Stato n. 8472/2019; Cons. di Stato n. 881/2020; T.a.r. Lazio n. 3679/2017. In dottrina Simoncini A., *L'algoritmo incostituzionale: intelligenza artificiale e futuro delle libertà*, in *BioLaw*, n. 1, 2019, p. 78; Manganaro F., *Trasparenza e digitalizzazione*, in *Diritto e processo amministrativo*, n. 1, 2019, p. 25 ss; Otranto P., *Riflessioni in tema di decisione amministrativa, intelligenza artificiale, legalità,* in *Federalismi.it* del 10 marzo 2021, n. 7, p. 203.
[442] EDPB, Guidelines 4/2019 on Articol 25 del 13 novembre 2019, p. 35.

Il Titolare dovrà, a tal fine, adottare misure appropriate per tutelare i diritti degli interessati garantendo agli stessi la possibilità di contestare la decisione assunta e il diritto di essere assistito da una persona, evitando che il trattamento sia gestito integralmente da un sistema informatico.
Il trattamento dovrà, inoltre, essere reso intellegibile al lavoratore affinché questi possa opporsi, esprimendo la propria opinione e contestando (ove lo ritenga) la decisione automatizzata assunta.
A tali misure possono esserne accostate ulteriori quali la pulizia dei *data set* al fine di garantire il principio di minimizzazione o l'impiego di tecniche di anonimizzazione o pseudonimizzazione dei dati trattati.

***

Concluso questo breve *excursus* sulla disciplina posta a tutela dei dati personali nel caso di trattamenti automatizzati o di profilazione, si vogliono esaminare gli adempimenti che andrebbero ottemperati qualora un datore di lavoro volesse monitorare i dipendenti al fine di valutarne la *performance*.
In questo caso il trattamento, volto a stimare il compimento di specifiche responsabilità connesse al ruolo assegnato o il raggiungimento di obiettivi prefissati, non può esimersi da una riflessione sulla possibilità di tracciare un profilo dei lavoratori osservati.
Il pericolo intrinseco, connesso all'attività di monitoraggio e valutazione, è quello di acquisire informazioni ultronee alla finalità sulla cui base elaborare profili dei prestatori validi per classificarli e assumere decisioni organizzative.
Il datore di lavoro dovrà, quindi, adottare opportune misure volte a garantire la legittimità del monitoraggio e del processo valutativo.

Qualora il datore di lavoro intenda monitorare i lavoratori per valutarne la *performance* lavorativa e ravvisi la possibilità di compiere un'attività di profilazione o decisionale automatizzata è tenuto, innanzi tutto, a rispettare la disciplina generale prevista dal GDPR per tutti i tipi di trattamento.
Devono, quindi, essere definite in modo chiaro le finalità di trattamento e queste devono essere proporzionate e necessarie al medesimo.
Deve, inoltre, essere indicata la base giuridica del trattamento che, nel caso della valutazione della *performance*, si fonda nel contratto di lavoro individuale o nei contratti collettivi. I dati raccolti devono, quindi, rispettare i criteri valutativi sanciti a livello individuale o collettivo.
La raccolta dei dati deve essere limitata e adeguata alla finalità dichiarata.
Il trattamento deve, quindi, tenere conto delle attività rilevanti per il raggiungimento degli obiettivi in relazione alle quali le informazioni raccolte devono essere non eccedenti.
I dati personali utilizzati nei processi di valutazione devono essere adeguati, ovvero esatti, e aggiornati regolarmente. Per far ciò, i dati devono essere accessibili ai lavoratori affinché ne possano avere contezza e ne possano chiedere la rettifica o la cancellazione se inesatti.
La necessità di poter correggere e adeguare i dati è tanto maggiore quanto più il processo di valutazione risulta automatizzato. Contrariamente, il processo di analisi produrrebbe risultati fallaci elaborati sulla base di *data set* viziati.
Il datore di lavoro deve, inoltre, informare i dipendenti - in modo trasparente e completo - che sono sottoposti a un monitoraggio compiuto con strumenti tecnologici e che i dati acquisiti verranno analizzati mediante processi completamente automatizzati.
Nella misura in cui l'esercizio dell'attività valutativa si basi su una specifica tecnologia, la raccolta dei dati deve risultare necessaria, proporzionata e attuata nel modo meno invasivo possibile.

Il processo di osservazione non dovrebbe, per esempio, basarsi su una sorveglianza costante delle attività compiute in ambienti digitali. Parimenti il trattamento di elaborazione dati dovrebbe limitare il campo di analisi agli obiettivi dichiarati o vincolare i risultati attenuti alle finalità indicate.
Conseguentemente, non devono essere rese disponibili - in conformità con i principi di liceità e minimizzazione riconosciuti dall'art. 5 del GDPR - informazioni ultronee ed eccedenti all'attività valutativa della *performance*, ancorché rese intellegibili con l'elaborazione.
Anche il tempo di conservazione dei dati deve essere limitato e calibrato con le finalità individuate.
Il datore di lavoro deve, quindi, conservare i dati per il solo tempo necessario a compiere la valutazione della *performance* o a completare il ciclo di valutazione delineato.
Pertanto, la conservazione per un termine superiore deve essere adeguatamente motivata, come nel caso risulti necessaria per realizzare un piano di sviluppo pluriennale, e l'informativa dovrà indicare in modo chiaro che i dati saranno utilizzati anche per i processi secondari.
Il datore di lavoro deve consentire ai lavoratori di poter esercitare i propri diritti, compresi il diritto di accesso, di rettifica e di cancellazione.
Per tale ragione, prima di introdurre strumenti di monitoraggio o di analisi, dovrebbero essere presi in considerazione i rischi che questi trattamenti possono comportare alle libertà dei lavoratori e porre in essere tutte le misure idonee a mitigare l'impatto che questi possono avere sugli interessati.
I dati personali devono, infatti, essere protetti dal datore di lavoro attraverso specifiche misure di sicurezza, tecniche e organizzative, che li tutelino da un accesso non autorizzato.
In merito trovano rilievo i concetti di *privacy by design* e *privacy by default,* introdotti dall'articolo 25 del GDPR, la cui definizione è stata oggetto di importanti linee guida predisposte dall'European Data Protection Board[443].
Il datore di lavoro deve, quindi, predisporre adeguate misure tecniche e organizzative già nel momento in cui vengono programmati i trattamenti di monitoraggio e analisi della *performance*, anticipando il momento di tutela (*data protection by design).*
Il Titolare deve, inoltre, mettere in atto misure di sicurezza adeguate "*per garantire che siano trattati, per impostazione predefinita, solo i dati necessari per ogni specifica finalità di trattamento*" (art. 25 par. 2 GDPR) tenendo in considerazione la quantità dei dati raccolti[444], la portata del trattamento[445], il periodo di conservazione[446] e l'accessibilità[447].

---

443 Cfr. EDPB, Guidelines 4/2019 on Articol 25 del 13 novembre 2019. La definizione delle misure tecniche e organizzative da adottare è stata descritta dal EDPB mediante una serie di elementi.
In primo luogo, è necessario eseguire una valutazione relativa al progresso della tecnologia presente compiendo una valutazione dello Stato dell'arte. In secondo luogo, il Titolare del trattamento deve compiere una valutazione in merito all'implementazione dei costi virgola non solo economici nell'adottare le misure tecniche organizzative adeguate, ma anche in riferimento alle risorse umane e al tempo da impiegare.
Deve essere poi compiuta una valutazione in merito a "*nature, scope, context and purpose"* del processo e ai rischi che "*varyng likelihood an severity for rights and freedoms of natural persons posed by the processing*".
La conclusione determina la scelta delle misure da adottare in riferimento al grado di rischio che comporta il trattamento dei dati.
444 EDPB, Guidelines 4/2019 on Articol 25 del 13 novembre 2019, p. 11 in cui si legge "*only the amount of personal data that is necessary for the processing shall be processed*".
445 EDPB, Guidelines 4/2019 on Articol 25 del 13 novembre 2019, p.12 ove si legge "*Processing operations performed on personal data shall be limited to what is necessary*".
446 EDPB, Guidelines 4/2019 on Articol 25 del 13 novembre 2019, p.12 ove si legge "*If personal data is not needed after its first processing, then it shall by default be deleted or anonymized*".
447 EDPB, Guidelines 4/2019 on Articol 25 del 13 novembre 2019, p.12 in cui si legge "*The controller must limit who can have access to personal data based on an assessment of necessity, and also make sure that personal data is in fact accessible to those who need it, when necessary, for example in critical situations*".

L'impiego di nuove tecnologie da cui possono scaturire rischi elevati ai diritti e alle libertà degli interessati obbliga il datore di lavoro a compiere una preventiva analisi dei rischi e a redigere una valutazione d'impatto (DPIA), ai sensi dell'articolo 35 del Regolamento.
L'inserimento di nuovi dispositivi dotati di capacità di monitoraggio ed elaborazione coinvolge la gestione di un rischio che deve essere previamente individuato e valutato mediante un processo strutturato finalizzato a stimarne gli effetti.
La DPIA si propone, quindi, di individuare, descrivere e valutare gli esiti che potrebbero derivare da un trattamento compiuto con nuove tecnologie, al fine di fornire informazioni utili a mitigare le eventuali conseguenze negative.
In aggiunta a tali prescrizioni generali, il datore di lavoro è tenuto ad attuare le misure specifiche, indicate dall'art. 22 del GDPR, garantendo la trasparenza del trattamento di profilazione o decisionale automatizzato integrato al processo di valutazione della *performance*.
Dovrà, quindi, essere comunicata, congiuntamente all'esistenza di tali trattamenti, la logica sottesa al processo, nonché l'importanza e le conseguenze che la profilazione o la decisione automatizzata possono comportare.
Al fine di facilitare l'effettiva intellegibilità della logica utilizzata, data la complessità tecnica delle informazioni può risultare utile il ricorso a modelli esplicativi che supportino i lavoratori nella comprensione.
Il datore di lavoro dovrà, infine, assicurare che il trattamento automatizzato possa essere contestato e riesaminato garantendo l'intervento umano.
Il lavoratore deve, quindi, essere posto nella condizione di conoscere e comprendere come operi lo strumento di osservazione e analisi, così da poter esprimere la propria opinione e, ove lo ritenga, opporsi al fine di ottenere una revisione umana del profilo ottenuto o nella decisione assunta.

2. Il Decreto Trasparenza. Quali novità in tema di *privacy* sui sistemi decisionali o di monitoraggio automatizzati

In riferimento ai sistemi decisionali e di monitoraggio automatizzati si devono citare le novità introdotte dal D. Lgs n. 104 del 27 giugno 2022[448] relative ai nuovi obblighi informativi posti a carico del datore di lavoro in caso di utilizzo di tali sistemi.
Il Decreto, ponendosi in dialogo con il GDPR[449], è intervenuto introducendo un'ulteriore norma, l'art. 1bis del D. Lgs n. 152 del 1997[450], inerente agli obblighi informativi limitatamente all'utilizzo di sistemi di monitoraggio o decisionali automatizzati.
Gli spunti di riflessione sono molteplici.
In primo luogo, la delimitazione dell'ambito di applicazione della norma.
Al comma 1, in riferimento agli ulteriori obblighi informativi introdotti, si legge che "*il datore di lavoro o il committente pubblico e privato è tenuto a informare il lavoratore dell'utilizzo di sistemi decisionali o di monitoraggio*

448 Per un approfondimento anche bibliografico si rinvia a Carinci M. T., Giudici S., Perri P., *Obblighi di informazione e sistemi decisionali e di monitoraggio automatizzati (art. 1-bis "Decreto Trasparenza"): quali forme di controllo per i poteri datoriali algoritmici?,* in *Labor*, n. 1, 2023, pp. 7 ss.
449 Esigenza che si evince dallo stesso Decreto ove specifica che resta salva "*la configurabilità di eventuali violazioni in materia di protezione dei dati personali ove sussistano i presupposti di cui agli articoli 83 del Regolamento UE 2016/679 e 166 del decreto legislativo 30 giugno 2003, n. 196 e successive modificazioni*" e come confermato dal Garante per la Protezione dei Dati Personali nelle questioni interpretative e applicative in materia di protezione dei dati connesse all'entrata in vigore del decreto del 13.12.2022 visibili sul sito https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9844960.
450 In merito Rossilli B., *Obblighi informativi relativi all'utilizzo di sistemi decisionali e di monitoraggio automatizzati indicati nel decreto "Trasparenza"*, in *Federalismi.it*, Focus lavoro persona tecnologia. Paper del 5 ottobre 2022; Faioli M., *Trasparenza e monitoraggio digitale. Perché abbiamo smesso di capire la norma sociale europea*, in *Federalismi.it*, Focus lavoro persona tecnologia del 5 ottobre 2022, n. 25, pp. 104 ss.

automatizzati deputati a fornire indicazioni rilevanti ai fini della assunzione o del conferimento dell'incarico, della gestione o della cessazione del rapporto di lavoro, dell'assegnazione di compiti o mansioni nonché indicazioni incidenti sulla sorveglianza, la valutazione, le prestazioni e l'adempimento delle obbligazioni contrattuali dei lavoratori (…)".
L'articolo si lascia influenzare dalla proposta di Direttiva del lavoro sulle piattaforme digitali facendo riferimento ai due distinti sistemi elencati all'art. 6 par.1 lett. a) e b) della norma europea.
Ciò porta a riflettere su cosa si deve intendere per "*sistema decisionale automatizzato*" e per "*sistemi di monitoraggio automatizzati*", le cui definizioni sono state oggetto di chiarimenti da parte del Ministero del Lavoro con la Circolare n. 19 del 20 settembre 2022[451].
Per il Ministero, la norma individua due distinte ipotesi di utilizzo dei sistemi automatizzati. Nel primo caso, fa riferimento a strumenti abilitati a realizzare un procedimento decisionale che può condizionare il rapporto di lavoro. Nel secondo caso, il Ministero intende un controllo automatizzato dell'attività lavorativa, ove gli strumenti incidono su sorveglianza, valutazione e adempimento delle obbligazioni contrattuali dei lavoratori.
Per rientrare nel cono applicativo dell'art. 1bis tali strumenti devono essere funzionali a fornire informazioni rilevanti per l'esercizio dei poteri datoriali in vari ambiti del rapporto di lavoro, tra cui si annoverano: l'instaurazione o la cessazione del rapporto, l'assegnazione di mansioni, la sorveglianza, l'adempimento e la valutazione delle obbligazioni dei lavoratori.
La norma richiama, di fatto, l'elenco posto nell'allegato 3 della proposta di Regolamento sull'Intelligenza Artificiale[452].
Per definire correttamente l'ambito applicativo della norma si deve, inoltre, ricordare che l'art. 22 del GDPR pone il divieto di assumere decisioni completamente automatizzate nei confronti dei lavoratori, salvo che queste non siano necessarie per l'esecuzione del contratto.
Si può, dunque, presumere che l'ambito di operatività dell'art. 1bis si estenda ai sistemi decisionali automatizzati (anche supportati da IA) impiegati quale mero ausilio della determinazione datoriale e non in sostituzione della medesima.
Diversamente la rilevanza della disposizione risulterebbe estremamente limitata.
Per sistemi decisionali automatizzati si devono, così, intendere non solo quelli che prevedono un processo decisionale autonomo della macchina, come potrebbe essere un sistema di IA, ma anche i sistemi algoritmici automatizzati che elaborano decisioni sulla base di istruzioni preliminari e senza ulteriori interventi umani.

Il primo comma si chiude con il rimando allo Statuto dei lavoratori - "*resta fermo quanto disposto dall'articolo 4 della legge 20 maggio 1970 n. 300*" - aprendo la questione di una sovrapposizione, ancorché parziale, delle due discipline e della loro armonizzazione.
In forza di tale richiamo, ove il monitoraggio automatizzato rientri in uno dei casi per cui è necessario sottoscrivere un accordo con le organizzazioni sindacali (ex art. 4 comma 1 SL), il datore di lavoro dovrà fornire alle rappresentanze tutte le ulteriori informazioni previste dal Decreto Trasparenza.

---

451 Chiarimento che ha fatto seguito alla circolare INL n.4/2022 del 10 agosto 2022. Il Ministero è intervenuto definendo cosa si intende per sistema decisionale e di monitoraggio automatizzato individuando due distinte fattispecie. Nella **prima** vi rientrano *"quegli strumenti che, attraverso l'attività di raccolta dati ed elaborazione degli stessi effettuata tramite algoritmo, intelligenza artificiale, ecc., siano in grado di generare decisioni automatizzate".*
La **seconda fattispecie** riguarda, invece, *"le indicazioni incidenti sulla sorveglianza, la valutazione, le prestazioni e l'adempimento delle obbligazioni contrattuali dei lavoratori".*

452 Allegato 3 punto 4: "*Occupazione, gestione dei lavoratori e accesso al lavoro autonomo: a)i sistemi di IA destinati a essere utilizzati per l'assunzione o la selezione di persone fisiche, in particolare per pubblicizzare i posti vacanti, vagliare o filtrare le candidature, valutare i candidati nel corso di colloqui o prove; b)l'IA destinata a essere utilizzata per adottare decisioni in materia di promozione e cessazione dei rapporti contrattuali di lavoro, per l'assegnazione dei compiti e per il monitoraggio e la valutazione delle prestazioni e del comportamento delle persone nell'ambito di tali rapporti di lavoro*".

Le Parti sociali devono, quindi, poter accedere a tutti gli elementi indicati dall'art. 1bis così da valutare l'effettiva portata del trattamento compiuto, le cui implicazioni devono essere recepite e risolte nell'accordo ex art. 4 SL.
Nei casi in cui, invece, il monitoraggio automatizzato esuli dalle ipotesi del primo comma dell'art 4 SL (e non sussista la necessità di un accordo con le rappresentanze sindacali), in ogni caso il datore di lavoro dovrà fornire tutte le informazioni aggiuntive indicate al comma 2 del Decreto Trasparenza, oltre a quelle previste dalla normativa statutaria e *privacy*.
Il richiamo allo Statuto dei lavoratori, sembra, quindi formulato al fine di rimarcare la non fungibilità dei due distinti obblighi informativi: quello contenuto nell'art. 4 SL, inerente alle modalità d'uso degli strumenti, all'effettuazione dei controlli e al trattamento dei dati personali del lavoratore, e quello introdotto dal Decreto Trasparenza, relativo alle modalità di utilizzo di sistemi tecnologici automatizzati per l'esercizio dei poteri datoriali.

In riferimento ai contenuti, la norma prevede al secondo comma l'obbligo per il datore di lavoro o il committente di fornire ulteriori specifiche informazioni rispetto a quelle previste dagli articoli 13 e 14 del GDPR.
Così facendo, la norma richiama e acquisisce un principio fondamentale per il trattamento dei dati personali, ovvero quello di trasparenza. Per tutelare i diritti dell'interessato è, infatti, fondamentale conoscere la natura automatizzata del trattamento.
Il principio di trasparenza viene garantito attraverso un'informativa specifica e ulteriore rispetto a quelle previste dal GDPR e alle comunicazioni più strettamente inerenti al rapporto di lavoro.
Circostanza sottolineata anche dal Garante per la Protezione dei Dati personali per il quale l'art. 1 bis del d.lgs. n. 152/1997 ha introdotto obblighi informativi che "*in parte integrano, in parte specificano gli obblighi posti dagli artt. 13 e 14 del Regolamento (UE) 2016/679*"[453].

Tra le informazioni ulteriori che il datore di lavoro deve fornire all'interessato vi sono: gli aspetti del rapporto di lavoro sui quali incide l'utilizzo dei sistemi decisionali o di monitoraggio automatizzati; il funzionamento dei sistemi; i parametri principali utilizzati per programmare o addestrare i sistemi decisionali o di monitoraggio automatizzati, inclusi i meccanismi di valutazione delle prestazioni. Devono, inoltre, essere comunicate le misure di controllo adottate per le decisioni automatizzate, gli eventuali processi di correzione e il responsabile del sistema di gestione della qualità; il livello di accuratezza, robustezza e *cyber* sicurezza dei sistemi decisionali o di monitoraggio automatizzati e le metriche utilizzate per misurare tali parametri, nonché gli impatti potenzialmente discriminatori delle metriche stesse.

Il datore di lavoro dovrà, inoltre, specificare con maggior accuratezza altre informazioni già elencate dagli artt. 13 e 14 del GDPR come la logica[454] dei sistemi decisionali o di monitoraggio automatizzati e le categorie di dati trattati[455].
Tutte le informazioni ineriscono al funzionano dei sistemi automatizzati così da porre il lavoratore e le Parti sociali nella condizione di conoscere quali siano le finalità e le modalità del trattamento e, al

[453] Punto 4, nota del Garante del 24 gennaio 2023 "*Questioni interpretative e applicative in materia di protezione dei dati connesse all'entrata in vigore del d. lgs. 27 giugno 2022, n. 104 in materia di condizioni di lavoro trasparenti e prevedibili*" consultabile al *link:* https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9844960
[454] La cui indicazione, nell'impianto degli artt. 13 e 14, è espressamente richiesta nel caso di ricorso ai processi decisionali automatizzati, compresa la profilazione, di cui all'art. 22 GDPR.
[455] Nel GDPR l'indicazione della categoria dei dati trattati è specificamente prevista solo qualora i dati oggetto di trattamento non siano ottenuti presso l'interessato (art. 14, par. 1, lett. d), del Regolamento).

contempo, responsabilizzando il datore di lavoro ad attuare idonee misure di sicurezza, tecniche e organizzative.
La norma prevede, quindi, l'adozione di procedure in cui si dia evidenza di come il datore di si sia adoperato per ridurre al minimo i rischi connessi al trattamento automatizzato.
In tale prospettiva, il riferimento alle categorie dei dati trattati (comma 2 lettera d) appare un elemento fondamentale per valutare il rischio del processo decisionale o di monitoraggio automatizzato essendo distinte le misure di sicurezza da applicare in base alla natura dei dati acquisiti (comuni o particolari) o alla loro significatività (dati su larga scala).
Di rilievo è, inoltre, il riferimento ai parametri utilizzati per *"programmare o addestrare i sistemi automatizzati"* (comma 2 lettera d), previsione che introduce un chiaro riferimento ai sistemi di IA e al principio di *privacy by design* (ex art. 25 GDPR) portando a valutare il funzionamento del sistema sin dalla sua progettazione.
La norma introduce, con il riferimento alla comunicazione delle *"misure di controllo adottate" e degli eventuali "processi di correzione*" (comma 2 lettera e), un sistema di contradditorio non solo sulle misure di controllo adottate, ma anche i processi di correzione, prevedendo la possibilità di intervento umano.
La disposizione prevede, inoltre, che vengano comunicati "*il livello di accuratezza, robustezza e cybersicurezza dei sistemi" e "gli impatti potenzialmente discriminatori delle metriche stesse"* (comma 2 lettera f).
Prima della novella il lavoratore e le Parti sociali non potevano esercitare il diritto di accesso a tali informazioni. Il diritto di accesso come delineato dal GDPR non prevede, infatti, che vengano comunicati tali elementi, pertinenti a ponderare i rischi del trattamento e integrati nella valutazione di impatto (DPIA).

Il Decreto, prendendo in considerazione l'impatto che tali strumenti automatizzati possono avere sul trattamento dei dati personali del lavoratore, al comma 4 inserisce ulteriori adempimenti a tutela della *privacy* del lavoratore.
Predispone, in primo luogo, un'integrazione delle informative *privacy* (artt. 13 e 14 GDPR) e un aggiornamento del registro delle attività di trattamento (art. 30 GDPR).
In secondo luogo, nel rispetto del principio di responsabilizzazione, la norma richiama il dovere vigente in capo al datore di lavoro o il committente di effettuare un'analisi dei rischi e una valutazione d'impatto (art. 35 GDPR), nonché di consultare preventivamente il Garante per la protezione dei dati personali ove ricorrano i presupposti (art. 36 GDPR).
Ipotesi, quest'ultima interessante perché, mediante l'esercizio del diritto di accesso, il singolo lavoratore o le Organizzazioni sindacali possono attivare la procedura di consultazione del Garante.

Analizzando la norma, una novità assoluta del neo-delineato sistema informativo viene introdotta al comma 6 dell'art. 1bis.
Tutte le informazioni contenute dal comma 1 al 5 devono, infatti, essere comunicate dal datore di lavoro o dal committente ai lavoratori.
I soggetti tenuti a fornire le informazioni sui sistemi sono, dunque, il datore di lavoro congiuntamente al committente. Si amplia, pertanto, il numero di soggetti obbligati alla trasparenza del trattamento. Tali informazioni devono essere il più possibili intellegibili, dovendo essere fornite "*in modo trasparente, in formato strutturato, di uso comune e leggibile da dispositivo automatico*".
Il comma prosegue precisando che "*la comunicazione delle medesime informazioni e dati deve essere effettuata anche alle rappresentanze sindacali aziendali ovvero alla rappresentanza sindacale unitaria e, in assenza delle predette rappresentanze, alle sedi territoriali delle associazioni sindacali comparativamente più rappresentative sul piano nazionale".*
Si introduce, dunque, un'ulteriore novità, ampliando la platea di destinatari dell'informativa e coinvolgendo anche le Parti sociali.

La norma dà, quindi, attuazione al secondo coma dell'art. 80 del GDPR ove si legge che in tema di rappresentanza degli interessati che "*gli Stati membri possono prevedere che un organismo, organizzazione o associazione di cui al paragrafo 1 del presente articolo, indipendentemente dal mandato conferito dall'interessato, abbia il diritto di proporre, in tale Stato membro, un reclamo all'autorità di controllo competente, e di esercitare i diritti di cui agli articoli 78 e 79, qualora ritenga che i diritti di cui un interessato gode a norma del presente regolamento siano stati violati in seguito al trattamento*".
Il secondo comma dell'art. 80 del GDPR prevede, dunque, il diritto delle Parti sociali a essere informate, ampliando la portata del diritto di informativa in una dimensione collettiva e riconoscendo la possibilità di azione direttamente ai sindacati.
Il "nuovo" diritto/potere sindacale delineato dal Decreto Trasparenza risulta, inoltre, esercitabile non solo nei confronti del datore di lavoro, ma anche nei riguardi del committente.
Con queste novità la normativa apre una nuova prospettiva di tutela.
Nei casi in cui un'attività lavorativa venga appaltata è il committente che può assumere decisioni fondamentali, come l'impiego di piattaforme o *software*, senza figurare quale effettivo datore di lavoro.
Prima della novella si poneva il problema dell'assenza di una tutela collettiva, non essendo il sindacato l'interlocutore diretto del committente e risultando soggetto estraneo al rapporto. Il committente poteva, infatti, figurare quale unico Titolare del trattamento pur non essendo datore di lavoro diretto, con conseguente assenza di qualsiasi azione collettiva.
Queste limitazioni precludevano alle Parti sociali la possibilità di agire, rendendo difficoltosa anche una tutela individuale, data la posizione esposta in cui si poneva il singolo lavoratore.
La norma, riscontrato tale *vulnus* di tutela, delinea in maniera innovativa un nuovo diritto collettivo ampliando la platea dei soggetti attivi e passivi dell'informativa.

3. Alcune osservazioni conclusive

Lo sviluppo di tecnologie capaci di compiere trattamenti automatizzati e il loro impiego nell'ambito lavorativo incide inevitabilmente sulla tutela dei dati personali dei lavoratori[456].
Il lavoro ha oggi una realtà fluida alternandosi tra una dimensione analogica e una digitale, strutturandosi come una relazione non solo di soggetti, ma anche di dati.
Questi sono oggetto di plurimi trattamenti a partire dal primo contatto con il candidato fino alla risoluzione del rapporto di lavoro, in taluni casi completamente automatizzati nel loro processo elaborativo.
La tutela dei dati personali si delinea, quindi, come una salvaguardia dei diritti delle libertà dei lavoratori.
Proteggere la *privacy* dei lavoratori deve portare, però, ad un'opera di bilanciamento dei distinti interessi che consenta di agire nel contesto lavorativo odierno secondo una visione "realistica" di quelle che sono le tecnologie ormai diffuse negli ambienti di lavoro.
Appare, dunque, opportuno andare oltre la mera asserzione di principio di "tutelare la *privacy*", talvolta ricondotta ad un asettico adempimento burocratico che grava sul datore di lavoro e in una corrispondente fatua tutela del lavoratore.

[456] Sul tema della tutela dei dati dei lavoratori si citano tra i molti Ingrao A., *Il controllo a distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata,* Cacucci, Bari, 2018; Ricci M., Olivieri A. (a cura di), *La tutela dei dati del lavoratore. Visibile e invisibile in una prospettiva comparata,* Cacucci, Bari, 2022; Sitzia A., *Il diritto alla "privatezza" nel rapporto di lavoro tra fonti comunitarie e nazionali*, Cedam, Padova, 2013; Tullini P. (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore,* Giappichelli Editore, Torino, 2017; Tullini P. (a cura di), Web *e lavoro. Profili evolutivi e di tutela,* Giappichelli Editore, Torino, 2017.

Il ruolo che il Legislatore europeo intende attribuire ai diritti di informazione riconosciuti dal GDPR, con riferimento alla loro dimensione individuale, è quello di strumenti di compensazione dell'"asimmetria informativa" derivante dalle potenzialità insite nelle tecnologie digitali.
La trasparenza delle informazioni assume, pertanto, una funzione abilitante dei diritti dei lavoratori.
In tal senso si è mosso anche il Legislatore italiano con il Decreto Trasparenza del giugno 2022 in cui configura un diritto del lavoratore e dei suoi rappresentanti a essere preventivamente informato riguardo all'utilizzo di sistemi di monitoraggio e decisionali automatizzati.

In che termini si devono, però, prospettare questi diritti di informazione di "nuova generazione" ai fini della tutela dei lavoratori?
Si deve andare sicuramente oltre alla concezione di informazione come specificazione delle condizioni contrattuali, rispetto alle quali il lavoratore assume una posizione di mero destinatario passivo (art. 96 disp. at. Cod. Civ).
Si deve andar oltre anche ad una definizione di informazione come mero elemento di verifica, ossia come motivazione della decisione assunta. In questo caso, infatti, l'informazione sarebbe funzionale solo a un momento di controllo sulla legittimità dell'esercizio dei poteri datoriali e all'esercizio del diritto di difesa rispetto a provvedimenti illegittimi.
La trasparenza deve, quindi, essere intesa quale mezzo attraverso cui sostenere le capacità di autogestione del lavoratore, rafforzandone la capacità di tutela mediante lo strumento dell'informazione.
Da qui la necessità non solo di comunicare le informazioni, ma di renderle intellegibili attraverso un linguaggio chiaro e comprensibile supportato, ove necessario, da modelli.
La previsione di comunicare in modo trasparente le informazioni si può, però scontrare con la reale complessità tecnica delle nozioni che devono essere fornite.
Vi è, così, il rischio che tali obblighi informativi si traducano in meri oneri burocratici vigenti in capo al datore di lavoro (o ai committenti in forza del Decreto Trasparenza).
Adempimenti che potrebbero essere soddisfatti mediante la predisposizione di documenti, corretti sotto un piano tecnico-formale, ma senza alcuna significativa incidenza sul piano sostanziale sia per il singolo lavoratore che per i rappresentanti coinvolti.
Garantire la trasparenza del trattamento comporta, quindi, il dovere di informare preliminarmente gli interessati fornendo indicazioni in merito alla tipologia di trattamenti compiuti, ai fini individuati e agli eventuali rischi che da questi possono derivare.
Parimenti, anche il Decreto Trasparenza richiede che il dovere di informativa sia reso all'avvio del rapporto di lavoro o almeno 24 ore prima ove subentrino variazioni nell'utilizzo dei sistemi che incidano sulle condizioni di svolgimento dell'attività.

La tutela *privacy* si prefigura, dunque, come intervento *ex ante*, chiedendo al datore di lavoro di responsabilizzarsi e di valutare preventivamente all'inizio dei trattamenti i rischi che da questi possono discendere.
Tale sistema di tutele si inserisce, però, all'interno di un rapporto di durata (quello lavorativo) in cui il trattamento dei dati avviene di continuo per effetto della datificazione.
Una comunicazione preventiva potrebbe, così, non essere sufficiente a informare adeguatamente o tempestivamente i lavoratori su tutte le ricadute che un determinato trattamento può comportare.
Anche la valutazione dei rischi, compiuta a priori su quelli che sono dati "non autoevidenti" e potenzialmente "totipotenti", potrebbe non rilevare tutti i rischi e le implicazioni che un loro trattamento comporta.

Tale previsione porta ad un'ulteriore riflessione.
La valutazione dei rischi connessi al trattamento o l'incidenza di tali sistemi alle condizioni di lavoro è rimessa al giudizio del solo Titolare del trattamento (datore di lavoro o committente che sia).
Viene quindi affidata all'autonomia del Titolare, nel rispetto del principio di responsabilizzazione, la decisione in merito alle modalità, alle garanzie e ai limiti del trattamento dei dati personali.
Conseguentemente, anche la valutazione dei rischi connessi al trattamento e le informazioni da fornire sono rimessi all'esame (discrezionale) del Titolare.
Far valere il principio di responsabilizzazione potrebbe, così, celare alcune insidie, data la visione parziale con cui viene valutato il trattamento e considerando la particolarità delle relazioni di lavoro, ove il soggetto interessato figura quale parte più debole del rapporto.
I destinatari del trattamento risultano, infatti, soggetti passivi non solo del trattamento, ma anche della pianificazione dello stesso.
Fatto che può comportare un ulteriore squilibrio tra le parti coinvolte.
Questione rilevata anche dal Parlamento Europeo che, negli emendamenti[457] proposti nel dicembre 2022 alla Proposta di Direttiva sulle condizioni di lavoro mediante piattaforma, ha imposto l'obbligo alle piattaforme digitali di coinvolgere i rappresentanti dei lavoratori nell'adempimento dei loro doveri relativi alla valutazione di impatto (ex art. 35 del GDPR).
Previsione che cerca, quindi, di promuovere la cooperazione tra le parti, mitigando gli effetti di parzialità legati al principio di responsabilizzazione.

Si deve poi ragionare sugli effetti che un trattamento dati può avere, al fine di comprendere qual sia il limite dell'osservabilità degli *output* ottenuti con l'elaborazione.
Come si è avuto modo di esaminare nei capitoli precedenti, le potenzialità di analisi, favorite dalla datificazione del lavoro, permettono di monitorare e comprendere ogni aspetto dell'attività lavorativa svolta dai dipendenti negli ambienti digitali. Inclusi i "comportamenti" e gli "atteggiamenti", ovvero il modo in cui i singoli si rapportano con i colleghi e con l'organizzazione.
Tali osservazioni, rimesse ad un "occhio digitale" capace di tracciare profili sulla base di un'analisi inferenziale, portano a far riflettere sull'ampiezza del monitoraggio condotto per fini legittimi, quale può essere quello di valutare la *performance*.
Intercettare "comportamenti" e "atteggiamenti" dei lavoratori può, infatti, rientrare nell'ambito della valutazione professionale del lavoratore, ma anche travalicarla accedendo alla sfera personale e disvelando, per esempio, opinioni e preferenze.
In altre parole, osservare digitalmente un atteggiamento vuol dire valutare la professionalità di un lavoratore o, in tal modo, se ne viola la riservatezza?
Se, infatti, è pur vero che nel momento in cui si instaura un rapporto di lavoro il prestatore accetta inevitabilmente di poter essere osservato, la tecnologia offre una lente di ingrandimento la cui potenza può ledere la tutela dei dati personali.
La possibilità di ottenere dati sempre più accurati su come i lavoratori si comportano in ambienti digitali, giustificata da scopi legittimi e finalità trasparenti, può restituire informazioni che ricadono in una "zona grigia" ove il confine tra professionale e personale appare sfumato.
La raffigurazione dei lavoratori realizzata con l'analisi dei dati può, infatti, alterare la conoscenza delle caratteristiche professionali note al datore di lavoro e porre nella disponibilità di quest'ultimo informazioni afferenti alla sfera personale.

[457] Si vedano i nuovi Considerando 32ter, Considerando 38bis, Art. 6, paragrafo 5 bis, Art. 7, paragrafo 1, Art. 7, paragrafo 2 bis della Proposta di Direttiva.

Elaborare e correlale dati consente di ottenere un'interazione più articolata con i lavoratori facendo emergere inferenze non prevedibili e informazioni non ricercate, in quanto ignote *ex ante*.
La potenzialità di elaborazione sembra, quindi, delineare un'area dal confine incerto ove il controllo e la *privacy* potrebbero trovare a priori idonee giustificazioni che legittimano il trattamento dei dati, ma in cui la dignità e la riservatezza dei lavoratori potrebbero, di fatto, venire lesi.
E ancora più sfumato può apparire il perimetro di questa "zona grigia" ove la natura dei dati analizzati possa essere in partenza qualificata come "non personale"[458] (non ritenendo i dati acquisisti idonei a identificare o a rendere identificabile un soggetto) e manifestandosi tale solo a seguito dell'analisi inferenziale[459].

Vi è, infine, un'ultima questione connessa alla struttura personale delle tutele delineate nel GDPR.
Ci si domanda, infatti, se la conoscenza delle informazioni può effettivamente salvaguardare il lavoratore ove garantita a livello individuale.
Il sistema di tutele basato su limiti interni ed esterni all'esercizio dei poteri datoriali rischia, infatti, di essere superato, piuttosto che accompagnato, da una normativa che venga a fondarsi e che riconosca maggior rilievo ai valori personalistici del lavoratore, estromettendo la dimensione collettiva.
Un tale sistema individua, così, il lavoratore quale unico limite che interviene *ab externo* rispetto alle prerogative datoriali.
Il rinvio posto dalla norma statutaria alla tutela *privacy* potrebbe, in tal senso, depotenziare e limitare il contro bilanciamento alle prerogative datoriali invece che rafforzarlo.

Date le premesse l'ironia con cui Platone affermava *nempe ridiculum esset, custode indigere custodem*[460] sembra superata e porta lecitamente a domandarsi *quis custodiet ipsos custodes?*[461]

[458] Nel momento in cui i dati vengono "spersonalizzati", mediante tecniche di anonimizzazione (per una definizione si veda art. 2 punto 7 Direttiva UE 2019/1024) o pseudonimizzazione (ex art. 4 punto 5 GDPR) fuoriescono dalla nozione di "dato personale" che costituisce il campo di applicazione del GDPR. Pari effetto si ottiene qualora si proceda alla cifratura dei dati personali, indicata dal GDPR quale misura adeguata a garantire la sicurezza del trattamento (ex art. 32 par. 1 lett. a).
[459] Si rinvia in merito al capitolo 3.
[460] Platone, La Repubblica III, 403e.
[461] Giovenale, Satire VI, 48-49.

Capitolo 5
Limiti al potere di controllo tecnologico e tutele di nuova generazione

1. Rivoluzione tecnologica e rapporto di lavoro: criticità emergenti connesse all'esercizio del potere datoriale

La riflessione che intreccia le tematiche del lavoro con l'innovazione digitale è volta a comprendere le eventuali criticità che la rivoluzione tecnologica e la regolazione a questa connessa potrebbero porre ai diritti dei lavoratori e alla loro *privacy*.
La tecnologia digitale applicata al lavoro consente un controllo prima non possibile, in grado di dedurre specifiche caratteristiche professionali e personali del lavoratore sulla base di dati non immediatamente correlati alle stesse.
In forza di ciò, il potere di controllo si abilita di nuove capacità, modificando la propria natura e travalicando la tradizionale divisione tra poteri datoriali, sino ad assumere la forma di un nuovo "potere di controllo direttivo".

Proprio l'impatto dell'innovazione digitale sui rapporti di lavoro ha indotto i giuslavoristi a ricostruire e adattare le categorie note - quale il potere di controllo - al nuovo contesto odierno, lontano dall'impresa di tradizione fordista.
Parimenti ha spinto il Legislatore europeo e nazionale a intervenire in materia, cercando di adottare strumenti che siano capaci di uniformare la disciplina a fronte delle nuove esigenze di tutela.
In questo scenario si collocano le vicende connesse al controllo tecnologico e ai rischi conseguenti all'impiego di algoritmi e sistemi di IA, soprattutto in un contesto lavorativo.

Nei capitoli precedenti si è visto, però, come l'introduzione di sistemi algoritmici integrati al lavoro, accompagnata da un aumento delle misure di raccolta e sorveglianza dei dati e di una loro elaborazione, minacci i valori ricercati dalla disciplina del diritto del lavoro e acuisca le vulnerabilità dei lavoratori nel loro rapporto con la parte datoriale.

La disuguaglianza tra prestatori e datore di lavoro appare implementata dall'impiego di sistemi algoritmici o di Intelligenza Artificiale la cui logica può appare inaccessibile e inspiegabile. Contestualmente, il grado di subordinazione pare aumentare a mano a mano che i dati vengono raccolti in misura crescente ed elaborati attraverso logiche algoritmiche.
In particolare, nel secondo capitolo, analizzando le modalità di impiego di strumenti digitali per la gestione del personale e l'esecuzione delle prestazioni in ambienti virtuali, si sono sollevate preoccupazioni in relazione al controllo sproporzionato che può derivare dalle tecniche di *Data Analysis*.
Il rischio intrinseco rilevato è quello di travalicare la finalità per cui un controllo sui lavoratori può considerarsi legittimo, ai sensi dell'art. 4 SL, e di compiere un controllo sproporzionato e diretto su aspetti altamente sensibili, come le condizioni psico-fisiche di una persona.
Pericolo rintracciato soprattutto ove le analisi avvengano su dati "non autoevidenti" e le valutazioni compiute a priori sull'esigenza di sorvegliare possano rivelarsi fallaci.
Il controllo tecnologico diventa, quindi, una forma più sofisticata di sorveglianza, non limitandosi a un'osservazione diretta, come nel caso dello *screenshot* di un videoterminale, ma basandosi sul processo di elaborazione dei dati.

In tale contesto si rinnova il problema delle modalità di esercizio dei poteri datoriali e su come la normativa, *iure condito* e *iure condendo,* possa impattare sul loro esercizio.

Appare, infatti, necessario comprendere quale sia la modalità più efficace in cui esse possano manifestarsi, in ragione delle potenzialità concesse dalle nuove tecnologie abilitanti, tenendo contestualmente presente i vincoli che gli devono essere apposti quale contrappeso a tutela degli interessi dei lavoratori.
Se il potere di controllo muta, ibridandosi con il potere direttivo, conseguentemente devono variare, adeguandosi, le tutele dei lavoratori, così da garantirne i diritti anche di fronte alle nuove esigenze.

La riflessione porta a ponderare non solo sull'opportunità di una partecipazione dei lavoratori alla programmazione di tali poteri, mediante l'elaborazione di modelli che ne procedimentalizzino l'esercizio, ma anche gli esiti che la loro applicazione può addurre.

Ci si domanda, quindi, quali siano le tutele che abbiano il potenziale di modellare (e limitare) la potestà datoriale che deriva dall'integrazione della tecnologia.

2. Tutela del lavoratore digitale e risposte regolative *de iure condito*. Il nuovo articolo 4 SL e controllo dei lavoratori mediante strumenti di analisi anche di dati "non autoevidenti?"
L'*iter* di indagine compiuto ha posto in evidenza le potenzialità e i rischi connessi all'utilizzo di strumenti tecnologici sofisticati, capaci di analizzare dati e di acquisire informazioni non immediatamente comprensibili.

"*Strumenti di data analytics o machine learning, reti neurali, deep-learning*"[462], ove impiegati in contesti lavorativi, possono determinare un elevato livello di rischio per i diritti e le libertà dei prestatori perché capaci di disvelare dati personali (anche eccedenti l'ambito strettamente professionale) e di compiere trattamenti (pure integralmente automatizzati) in grado di tracciare la prestazione e delineare un profilo digitale del prestatore.

L'ambiguità maggiore e il rischio che ne consegue in un approccio *Data-Driven* è l'apparente neutralità di alcune categorie di dati, qui definiti come "non autoevidenti", capaci di restituire informazioni personali - professionali e non - solo a seguito della loro interpretazione.

Orbene, quando strumenti sofisticati di analisi vengono applicati in contesti lavorativi, ci si è chiesti se il nuovo articolo 4 SL legittimi un controllo "mirato" sui prestatori.

L'art. 4 SL, come riscritto nel 2015, separa, innanzi tutto, le finalità che legittimano l'acquisizione dei dati personali dal loro utilizzo.

La legittimità dell'interesse datoriale a compiere un controllo (pur sempre e solamente indiretto) deriva, pertanto, dalle esigenze qualificate dall'art. 4 SL.
La norma impone, così, una preliminare analisi sui motivi che giustificano l'acquisizione dei dati, quale può essere quella organizzativa finalizzata a valutare la *performance*.

L'articolo procedimentalizza il potere datoriale imponendo una verifica *ex ante* sulla tecnologia impiegata e sui motivi che ne autorizzano l'installazione.

[462] Utilizzando il lessico impiegato dal Legislatore nel D. Lgs. 27 giugno 2022, n. 104 in materia di condizioni di lavoro trasparenti e prevedibili, c.d. Decreto Trasparenza.

Nel caso della valutazione della *performance* mediante strumenti di analisi, il controllo che ne deriva dal loro utilizzo è ammissibile ove sia legittima l'esigenza di installazione di *tools analytics*.

Dal vaglio di legittimità preventivo appare, però, sottratta quella parte di trattamenti che, pur accompagnando la decisione datoriale di compiere un controllo a distanza per soddisfare esigenze aziendali determinate, non consenta una scelta preliminare - certa e selettiva - degli *output* acquisibili.

Come si è avuto modo di osservare nel capitolo 2.2, ove mediante distinti casi di studio si è cercato di compiere una sorta di "*crash test*" della normativa giuslavoristica, l'esercizio del potere di controllo in contesti digitali viene esercitato sempre più quando i dati sono elaborati (e dunque utilizzati) e non quando questi sono acquisiti
Verificare l'esistenza e la fondatezza di un'esigenza datoriale può risultare, in tal modo, parziale di fronte a dati dal valore apparentemente neutro, ma potenzialmente capaci di disvelare informazioni personali.

L'impiego di sistemi di analisi, da cui deriva l'autentica forza del monitoraggio, sposta il tema della legittimità del controllo compiuto dall'acquisizione all'elaborazione (e dunque utilizzo) dei dati trattati e alle tutele *privacy* richiamate dal terzo comma dell'art. 4 SL.

In particolare, la natura dei dati trattati e le funzionalità di elaborazione associate a questi sistemi – automatiche e/o di profilazione - sollevano riflessioni critiche in merito al trattamento di informazioni attinenti alla sfera personale - ma non extra-lavorativa - dei lavoratori, nonché alla proporzionalità del loro impiego.
Questa valutazione deve tenere in considerazione, infatti, anche i limiti posti dall'art. 8 SL, il cui divieto vale non solo per le indagini compiute in maniera diretta, ma anche per quelle svolte attraverso trattamenti leciti capaci, però, di raccogliere in maniera esplorativa i dati sui lavoratori.
L'attinenza del fatto indagato all'attitudine professionale del lavoratore rappresenta il punto di discrimine tra una indagine vietata e una lecita.
Anche nel caso dell'art. 8 SL il freno posto "dall'attitudine professionale" potrebbe, però, perdere di incidenza data l'attenzione posta dalla norma al momento in cui i dati vengono acquisiti.
Ciò potrebbe escludere dal vaglio critico i dati "non autoevidenti", non classificabili a priori come capaci di disvelare "opinioni" dei lavoratori.

La questione si sposta, pertanto, sulle tutele contenute nella normativa *privacy* aprendo, così, nuovi scenari di responsabilizzazione in capo al datore di lavoro, il quale non solo deve valutare la fondatezza delle esigenze per l'installazione di strumenti di controllo (indiretto), ma anche la legittimità del trattamento che questi possono compiere.

Qualora, infatti, il controllo a distanza sia in grado di restituire un profilo digitale del lavoratore destinato a valutare l'esecuzione della prestazione, oppure l'attitudine professionale o il rendimento, la legittimità nell'utilizzo dei dati è subordinata all'esistenza di una finalità di trattamento, necessariamente connessa all'esigenza aziendale che ne consente l'acquisizione

Il controllo mirato sui prestatori ai fini di valutarne la *performance* sarebbe, dunque, legittimo ove la finalità del trattamento sia riconducibile allo scopo organizzativo e i dati - non più solo acquisiti, ma anche utilizzati - siano limitati a quelli esclusivamente necessari a realizzare la valutazione.

Un controllo specifico dei lavoratori sarebbe, così, ammissibile ove la peculiare esigenza datoriale non possa essere raggiunta con alcun altro strumento di analisi che compia un monitoraggio di natura meno invasiva, tenute in considerazioni le concrete modalità di esercizio del potere datoriale di controllo.

Il controllo che deriva dalle tecniche analitiche deve risultare, pertanto, proporzionato, bilanciando in maniera equa gli interessi datoriali e ai diritti dei lavoratori interessati.

La questione in merito alla legittimità del trattamento si risolve, così, all'interno del perimetro tracciato dall'art. 4 SL che, integrato dalla normativa *privacy* a cui rinvia, sposta l'attenzione da un regime "statico" di verifica preliminare - finalizzata ad autorizzare uno strumento – ad un accertamento "dinamico" sull'esecuzione di un trattamento.
La normativa *privacy* influenza, in tal modo, l'esercizio del potere datoriale di controllo, imponendo il rispetto di obblighi informativi e di principi che responsabilizzano il datore di lavoro in quanto titolare del trattamento.
Tale prospettiva consente di strutturare una valutazione prognostica di rischio in riferimento ai dati che possono non essere ancora acquisiti, ma sono potenzialmente "acquisibili" con sistemi di *Data Driven*.

Il fulcro di tutela della "riservatezza" del lavoratore è, dunque, rappresentato non più solo dal divieto di compiere un controllo diretto sulla prestazione lavorativa, ma dal rispetto dei principi e dalle tecniche di tutela dei dati.

Il principio di "*accountability*", in particolare, pone in capo al datore di lavoro un dovere di analisi critica in relazione a quelli che possono essere gli i dati acquisibili, le finalità di utilizzo, la minimizzazione dei dati impiegati e la proporzionalità dei trattamenti compiuti per realizzare i propri interessi.

Una responsabilità che sarà tanto maggiore quanto più alto è il rischio connesso al trattamento, come nel caso in cui siano adoperati sistemi automatizzati o di profilazione[463].

L'impiego di strumenti di analisi che consentano il controllo delle prestazioni deve, dunque, impedire l'acquisizione di dati che contengano (o possano contenere) informazioni eccedenti rispetto alla sfera professionale e allo scopo per le quali il trattamento viene attuato.

Tale riflessione interessa non solo i dati personali, ma anche (e soprattutto) quelli particolari dei lavoratori[464], quale può essere il grado di soddisfazione.

---

463 Si ricorda, infatti, che il GDPR non vieta l'attività di profilazione ove il trattamento automatizzato sia necessario per la conclusione o l'esecuzione di un contratto tra l'interessato e il Titolare del trattamento (art. 22 par. 2 GDPR).

464 Il GDPR, infatti, consente il trattamento dei dati particolari ove questo sia "*necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, (…)*" (art. 9 comma 2 GDPR).
Anche l'Autorizzazione generale del Garante n. 146 del 5 giugno 2019 per la protezione dei dati personali ammette il trattamento dei dati particolari ove funzionale alla gestione, instaurazione e cessazione della relazione lavorativa. Garante *Privacy*, *Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati*, *Deliberazione n. 53 del 23 novembre 2006* e successivo *Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101.*

Calando tali principi richiamati nel caso di specie di valutazione della *performance*, il controllo compiuto con *tools analytics* sulle prestazioni digitali risulterebbe proporzionale se:

- la finalità di trattamento sia determinata a priori e risulti connessa alle esigenze datoriali indicate dall'art. 4 comma 1 SL (nello specifico quella organizzativa);
- tali dati (personali o particolari) risultino tutti attinenti alla sfera professionale del prestatore (ex art. 8 SL);
- non sussistano altri strumenti di analisi che possano compiere un monitoraggio meno invasivo di quello posto in essere con i sistemi scelti;
- il trattamento dei dati avvenga nel rispetto della normativa *privacy*;
- i dati acquisiti (prima) e utilizzati (poi) siano selezionati in maniera da minimizzarne l'impiego a solo quelli strettamente necessari per realizzare la finalità di trattamento connessa all'esigenza datoriale;
- ove vengano impiegati processi automatizzati, anche di profilazione, siano adottate tutte le misure idonee a consentire al prestatore di richiedere e ottenere l'intervento umano, di esprimere la propria opinione e di contestarne la decisione (art. 22 par. 3 GDPR);
- ove vengano impiegati processi decisionali e di monitoraggio automatizzati, vengano fornite tutte le informazioni introdotte dal D. Lgs. 27 giugno 2022, n. 104 in materia di condizioni di lavoro trasparenti e prevedibili, c.d. Decreto Trasparenza.

Il mancato rispetto di ognuna di queste condizioni rende il trattamento (e il controllo indiretto conseguentemente esercitato) illegittimo e, dunque, vietato.
Il nuovo articolo 4 SL legittima, quindi, un controllo "mirato" della *performance* nel senso di circoscritto alle esigenze e finalità e condotto sui soli dati pertinenti allo scopo prefissato.
Rimarrà, invece, precluso un controllo che esegua un tracciamento della prestazione che ecceda per volume, tipologia o durata di dati raccolti le finalità di valutazione

Pertanto, ove l'acquisizione di informazioni a seguito dell'elaborazione di dati, anche "non autoevidenti" risulti sproporzionata rispetto allo scopo prefissato di valutazione della *performance*, l'analisi dovrà considerarsi vietata.

La limitazione della finalità di trattamento vincola, inoltre, l'utilizzo delle informazioni (acquisite o acquisibili) circoscrivendone l'impiego.
Per tale ragione, l'utilizzo di dati per scopi distinti da quelli dichiarati preliminarmente nell'informativa resa ai lavoratori deve ritenersi precluso.
Non potranno, per esempio, impiegarsi informazioni (anche ottenute dall'elaborazione di dati "non autoevidenti") per fini disciplinari[465] ove la finalità di trattamento dichiarata, connessa allo scopo organizzativo, sia solo quella di valutare la *performance*.

I principi posti a tutela dei dati personali operano, così, in combinato disposto con quelli giuslavoristici.
Conseguentemente, la valutazione del rischio rinvia ad una ponderazione in merito al modo in cui il controllo indiretto, derivante dal trattamento dei dati, si concretizza obbligando il datore di lavoro ad

[465] Cfr. Ingrao A., *Il controllo a distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata*, Cacucci Editore, Bari, 2018 pp. 179 ss.

attuare misure tecniche e organizzative affinché il monitoraggio del comportamento solutorio del lavoratore non divenga pervasivo[466].

Tali principi trovano applicazione anche per le altre esigenze di controllo, ex art. 4 comma 1 SL, come nel caso di installazione di dispostivi di monitoraggio volti a proteggere la salute e sicurezza dei lavoratori. Anche in tali ipotesi, il datore di lavoro è legittimato a eseguire accertamenti per tutelare i propri preposti, ma senza procedere ad una vigilanza diretta sulla loro salute.
Questa valutazione dovrà essere ancora più accurata ove i dispositivi impiegati (quali possono essere i *wearable device*) vengano impiegati per finalità cumulative e contestuali come l'efficientamento dei processi e la prevenzione dei rischi sulla salute.
La responsabilizzazione del Titolare del trattamento si traduce nell'obbligo di valutare il rischio di lesione dei diritti fondamentali dei lavoratori e di predisporre misure idonee a prevenire o mitigare tale rischio.
Di conseguenza, il datore di lavoro dovrà dichiarare preliminarmente le finalità per cui intende utilizzare strumenti capaci di monitorare la salute dei lavoratori e circoscrivere i dati che questi possono restituire alle sole informazioni attinenti alle specifiche finalità. Ciò tenendo ben presente che le informazioni possono essere ricondotte ad una persona fisica anche solo a seguito dell'elaborazione.

La recente attenzione sugli strumenti informatici e sui trattamenti automatizzati che questi possono compiere ha sollevato riflessioni, sia a livello europeo sia nazionale, sul ruolo riservato agli interessati e su come questi possano intervenire in maniera più attiva a tutela dei propri diritti.
Ci si è accorti, infatti, che controlli eseguiti in maniera solo preliminare possono fornire una tutela parziale a chi è il soggetto passivo dei trattamenti automatizzati.

La necessità di procedere ad una verifica dinamica della tutela dei diritti degli interessati ha portato a sviluppare un approccio basato sulla valutazione del rischio.
Un sistema di garanzia "*risk-based*", qual è quello adottato dal GDPR e dal prossimo Regolamento sull'IA, implica una necessaria responsabilizzazione del soggetto che compie il trattamento, essendo colui che deve valutare il rischio e agire per limitarlo.
Non esige sempre, però, un corrispettivo ruolo attivo dell'interessato.

La strada intrapresa per sopperire a tale mancanza è stata quella di potenziare il diritto di informazione, imponendo ampli obblighi preventivi a carico del datore di lavoro, favorendo la trasparenza dei trattamenti.
Scelta condivisibile ove si consideri che la forza del nuovo potere "di controllo direttivo" del datore di lavoro deriva dall'opacità delle logiche delle scelte compiute dai sistemi automatizzati e dalla potenzialità di disvelare nuove informazioni.
Soluzione condivisa a livello europeo dal GDPR[467] dalla proposta di Direttiva sul lavoro mediante piattaforme e dalla proposta di Regolamento sull'IA.

Sulla stessa linea, anche il Legislatore nazionale, nel c.d. Decreto Trasparenza, si muove nella direzione di introdurre nuovi diritti di informazione a favore dei lavoratori e dei loro rappresentanti.

---

[466] In merito Alessandra Ingrao osserva che "*il controllo continuativo è contrario (…) al principio di minimizzazione dei dati che (…) al fine di salvaguardare la dignità umana dell'interessato del trattamento, postula che il potere di raccogliere dati altrui sia limitato al minimo, sia in relazione alla qualità di dati captata sia per quanto riguarda il periodo temporale in cui la raccolta si svolge*". Ingrao A., *Il controllo a distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata*, Cacucci Editore, Bari, 2018, 179.
[467] Si veda l'art. 22 sui processi decisionali automatizzati.

Sembra, così, variare parzialmente la struttura delle tutele giuslavoristiche, non più basata esclusivamente sul rispetto di norme imperative, che impongono limiti precisi e preordinati al potere datoriale, in favore di obblighi di natura informativa che comunichino al lavoratore (o ai suoi rappresentanti) i rischi che i trattamenti possono apportare.

La limitazione del potere di controllo datoriale divine, così, più flessibile, imponendo una costante "autoverifica" al datore di lavoro responsabilizzato nel proprio ruolo di titolare.
"Autoverifica" che non deve, però, essere "autoreferenziale", venendo potenziato l'intervento dei lavoratori o delle Parti Sociali nel processo di analisi del rischio e di adozione di rimedi volti a limitarlo.
Lo scopo è quello di consentire la reale comprensione del fine che si intende realizzare con il trattamento e di limitare i dati alle sole informazioni (acquisite o acquisibili) pertinenti allo scopo dichiarato.

La dimensione di tutela data dai "nuovi" diritti di informazione ricade, in ogni caso, nello spazio di legittimità tracciato dalla disciplina lavoristica specifica applicabile in materia, ossia dalla norma statutaria. Questo significa che il trattamento dei dati personali rimane governato dall'art. 4 SL (*in primis*) e dalle regole sulla protezione dei dati personali a questo integrative[468].

Ciò non esclude, però, che il Legislatore nazionale, preso atto delle potenzialità intrinseche nei nuovi strumenti digitali - ormai diffusi negli ambienti di lavoro - possa modificare il testo dell'art. 4 SL prevedendo che la verifica delle esigenze datoriali di controllo avvenga non solo preliminarmente all'acquisizione dati, ma anche durante il trattamento.
In tal modo, il potere datoriale di controllo vedrebbe una procedimentalizzazione che trascende il solo momento di istallazione degli strumenti, prevedendo una fase (necessaria) di dialogo, con il lavoratore e le Parti Sociali, anche durante l'utilizzo dei dati.

3. Tutela del lavoratore digitale e risposte regolative *de iure condendo*

Per rispondere al quesito su quali possano essere gli strumenti capaci di mitigare le nuove manifestazioni del potere datoriale la riflessione non può che iniziare delle soluzioni proposte dalle norme europee di prossima emanazione quali la proposta di Regolamento sull'IA e dalla proposta di Direttiva sul lavoro mediante piattaforme.
L'analisi proseguirà soffermandosi su alcuni aspetti che l'autrice considera particolarmente rilevanti per rinvenire tutele idonee a bilanciare il potere di controllo direttivo con gli interessi dei lavoratori.

3.1. La proposta di Regolamento sull'IA

Una possibile soluzione alla nuova manifestazione del potere datoriale è stata rintracciata nell'esigenza di stabilire norme comuni così che l'impiego della tecnologia risulti equilibrato, corretto e capace di tutelare i diritti fondamentali dei lavoratori.
Da qui l'utilizzo dello strumento del Regolamento europeo per regolare nuovi settori, come quello dell'Intelligenza Artificiale[469].

---

[468] Lo stesso «decreto trasparenza» richiama l'art. 4 St. lav.

[469] Per un approfondimento si rimanda a Peruzzi M., *Intelligenza Artificiale e lavoro. Uno studio su poteri datoriali e tecniche di tutela,* Giappichelli Editore, Torino, 2023; Alaimo A., *Il Regolamento sull'Intelligenza Artificiale,* in *Federalismi.it*, n. 25, 2023, pp. 132 ss; Loi P., *Il rischio proporzionato nella proposta di regolamento sull'IA e i suoi effetti nel rapporto di lavoro*, in *Federalismi.it*, n.4, 2023, pp. 239 ss; Lo Faro A., *Algorithmic Decision Making e gestione dei rapporti di lavoro: cosa abbiamo imparato dalle piattaforme*, *in Federalismi.it*, n. 25, 2022, pp. 201 ss; Lamberti F.*, La proposta di regolamento UE sull'Intelligenza Artificiale alla prova della privacy*, in *Federalismi.it*, del 29 giugno 2022, pp. 1 ss; Tullini P., *La Direttiva Piattaforme e i diritti del lavoro digitale,* in *Labour & Law Issues (LLI), vol. 8, n. 1,*

L'*iter* di approvazione del Regolamento sull'IA (AIR), la cui proposta risale ad aprile 2021[470], risulta ormai al termine.
Il 14 giugno 2023 il Parlamento europeo ha, infatti, approvato *AI Act* emendando il testo proposto dalla Commissione europea del 21 aprile 2021. Prima che il progetto normativo diventi legislazione la proposta dovrà essere discussa dal Consiglio dell'Unione europea e dalla Commissione europea.
Il 9 dicembre 2023 la presidenza del Consiglio e i negoziatori del Parlamento europeo hanno raggiunto un accordo provvisorio sulla proposta relativa a regole armonizzate sull'intelligenza artificiale (IA).
Rispetto alla proposta iniziale della Commissione, i principali nuovi elementi dell'accordo provvisorio sono stati elencati dal Comunicato stampa del Consiglio dell'UE del 9 dicembre 2023 e possono essere sintetizzati come segue:

- *"regole sui modelli di IA per finalità generali ad alto impatto che possono comportare rischi sistemici in futuro, nonché sui sistemi di IA ad alto rischio*
- *un sistema di governance riveduto con alcuni poteri di esecuzione a livello dell'UE*
- *ampliamento dell'elenco dei divieti, ma con la possibilità di utilizzare l'identificazione biometrica remota da parte delle autorità di contrasto negli spazi pubblici, fatte salve le tutele*
- *una migliore protezione dei diritti tramite l'obbligo per gli operatori di sistemi di IA ad alto rischio di effettuare una valutazione d'impatto sui diritti fondamentali prima di utilizzare un sistema di IA".*[471]

Il comunicato prosegue specificando le tempistiche del prossimo Regolamento IA, prevendendo che si applichi due anni dopo la sua entrata in vigore salvo alcune eccezioni per disposizioni specifiche.
Le prossime tappe vedranno la prosecuzione dei lavori a livello tecnico per definire i dettagli del nuovo regolamento. Una volta conclusi i lavori, il testo verrà sottoposto ai rappresentanti degli Stati membri per l'approvazione.
Il testo integrale definitivo prima dell'adozione dovrà, inoltre, essere confermato da Consiglio dell'UE e Parlamento europeo e sottoposto alla messa a punto giuridico-linguistica.

Si deve tenere presente che la disciplina del AIR non risulta concepita in uno spazio di diritto "vuoto" potendosi avvalere dell'integrazione di altre discipline poste a latere[472], quali il GDPR, trovando un ulteriore riferimento integrativo negli interventi delle Parti sociali europee e nazionali.
La realizzazione di una strategia di IA affidabile richiede, infatti, la tessitura tra diversi fini che costituiscono l'intreccio fra diritto di protezione dei dati, diritto del lavoro e altre norme di matrice sociale, comprese quelle delineate dal dialogo delle Parti Sociali europee e nazionali.

2022, R 43 – R 56; Tullini P., *La nuova proposta europea sull'intelligenza artificiale e le relazioni di lavoro*, in *Trabajo, Persona, Derecho, Mercados,* n. 5, 2022, pp. 99-108; Natali L. C., *Intelligenza artificiale e impatto sul lavoro, in Diritto e Pratica del Lavoro,* n. 23, 1° giugno 2023, pp. 1446 ss; Adams Prassl J.*, Regulating Algorithms at Work: Lessons for a 'European Approach to Artificial Intelligence'*, in *European Labour Law Journal*, vol. 13, n. 1, 2022, consultabile al *link* https://journals.sagepub.com/doi/full/10.1177/20319525211062558; Iodice R., *La proposta di Regolamento UE sull'Intelligenza Artificiale: quali implicazioni sul versante giuslavoristico?,* in *IANUS*, n. 24, 2021, pp. 55 ss; Piccinini I., Isceri M., *IA e datori di lavoro: verso una e-leadership?,* in *Lavoro Diritti Europa*, n. 2, 2021, pp. 1 ss; De Stefano V.; *The EU Commission's proposal for a Directive on Platform Work: an overview;* in *Italian Labour Law e-Journal,* n. 1, vol. 15, 2022, pp. 1 ss.

470 La proposta per il Regolamento sull'I.A. può essere visionata al link: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52021PC0206.

471 Comunicato stampa del Consiglio dell'UE del 9 dicembre 2023 consultabile sul sito: https://www.consilium.europa.eu/it/press/press-releases/2023/12/09/artificial-intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai/

472 Ulteriori integrazioni potranno pervenire dai nuovi progetti normativi come il *Data Governance Act* (DGA), il *Digital Services Act* (DSA) e il *Digital Markets Act* (DMA).

Coerentemente, l'Accordo quadro europeo sulla digitalizzazione del 2 giugno 2020[473] rinvia alle Parti Sociali nazionali la trasposizione del documento al fine di definire, mediante lo strumento della contrattazione collettiva, una disciplina di maggior tutela.
In merito, si segnalano alcuni primi riferimenti all'impiego dell'IA sui luoghi di lavoro nella contrattazione collettiva nazionale come, per esempio, è avvenuto nel Contratto delle telecomunicazioni, rinnovato nel 2020[474], che contiene un riferimento a linee guida sull'utilizzo di sistemi di IA per stipulare accordi a livello aziendale.
Norme sull'informazione, consultazione, negoziazione e persino nuove prassi partecipative[475] possono, quindi, trovare adeguata collocazione nei testi di legislazione sociale e nel dialogo sociale, ove risultino carenti nel testo di regolamentazione europeo.

Analizzando la struttura della proposta di Regolamento sull'IA, si osserva che questa segue un approccio regolativo *omnibus* "orizzontale"[476] basato sul rischio, al pari del GDPR[477], distinguendone tre differenti tipi: inaccettabile, alto e basso.
Ciò significa che il AIR interviene sulle modalità di utilizzo della tecnologia, prevedendo una differente regolamentazione a seconda della categoria del rischio.
La proposta di Regolamento prefigura per primi i sistemi di IA a rischio inaccettabile il cui utilizzo è vietato.
Successivamente descrive i sistemi ad alto rischio, il cui utilizzo è condizionato al rispetto di determinati requisiti la cui conformità viene valutata *ex ante*.
Infine, individua i sistemi a basso rischio il cui uso è consentito senza alcun tipo di restrizioni e il cui impiego è, però, legato a obblighi di trasparenza e di conformità con il GDPR.
Tra i sistemi considerati ad alto rischio rientrano anche quelli applicabili in ambito lavorativo che il AIR menziona in due punti utilizzando i termini "*nel settore dell'occupazione, nella gestione dei lavoratori e nell'accesso al lavoro autonomo*".
Tali riferimenti risultano esterni all'articolato del Regolamento, venendo menzionati nel 36esimo Considerando e nel punto 4 dell'allegato 3.
La proposta di Regolamento prevede che tutti i sistemi di IA ad alto rischio debbano possedere dei requisiti[478], ponendo precisi obblighi in capo al soggetto che sviluppa o commercializza il sistema, ossia a colui che fornisce il sistema di IA.

---

473 L'accordo del 2020 mette in evidenza come il coinvolgimento dei lavoratori e delle Parti Sociali, attraverso una loro consultazione tempestiva, sia importante per ottenere il consenso dei lavoratori all'utilizzo della tecnologia digitale.
474 CCNL Telecomunicazioni del 12.11.2020. Art. 57 "*Nuove tecnologie e tutela dei diritti dei lavoratori*".
475 In merito parte della dottrina ha parlato di *Participatory Design,* proponendo una logica collaborativa e di dialogo tra lavoratori (o loro rappresentanti) e datori di lavoro per l'utilizzo di strumenti algoritmici o di IA. Cfr. Bossen C., Dindler C., Iversen S. O., *Evaluation in participatory design: a literature survey*, in *Proceedings of the 14th Participatory Design Conference*, vol.1, 2016, pp. 151-160. Alcuni autori suggeriscono di sperimentare la tecnica della regolazione mista basata sulla combinazione di regole imperative e reattive. Le regole del primo tipo dovrebbero mirare a garantire i diritti fondamentali dei lavoratori, mentre le altre dovrebbero mirare a garantire la "libertà positiva" dei lavoratori potenzialmente inclusa nei nuovi modelli di lavoro. In tal senso Senatori I., *Regulating the Employment Relationship in the Organization 4.0: Between Social Justice and Economic Efficiency*, in *The Future of Work. Labour Law and Labour Market Regulation in the Digital Era* a cura di Perulli A., Treu T., Wolters Kluwer, Paesi Bassi, 2021.
476 Al pari della proposta di Direttiva per responsabilità di danni extracontrattuali derivanti dall'uso di sistemi di IA presentata a fine settembre 2022 dalla Commissione europea non è regolata per settori.
477 La disciplina proposta dal AIR mutua dal GDPR alcuni elementi fondamentali quali: l'approccio fondato sul rischio secondo una prospettiva di gravità crescente, la valutazione d'impatto per la valutazione del rischio, la previsione di doveri di trasparenza nei confronti degli utenti, la previsione di codici di condotta in funzione co-regolativa; la comunicazione obbligatoria degli "incidenti" potenzialmente pregiudizievoli.
478 I requisiti di utilizzabilità dei sistemi ad alto rischio sono i seguenti: dati per l'apprendimento e la convalida del sistema; requisiti di documentazione tecnica; trasparenza e informazione; supervisione umana; *cyber security*. L'obbligo del rispetto di tali requisiti ricade sulla figura del *provider*, con riferimento alla fase di *design* e di *development* e, quindi, prima dell'immissione sul

Quest'ultimo deve sottoporre il sistema a una procedura di valutazione di conformità prima che il sistema di IA sia utilizzato e immesso sul mercato, analizzando i rischi e la qualità.
In particolare, l'art. 14 del AIR prevede che i sistemi di IA debbano essere progettati e sviluppati in maniera da consentire un effettivo e continuo controllo umano.
Agli utilizzatori spetta, invece, l'obbligo di attenersi alle istruzioni d'uso, di supervisione e monitoraggio, nonché di informare ove si manifestino malfunzionamenti o incidenti nell'impiego.
La normativa della proposta di Regolamento sull'IA appare, così, una disciplina che riecheggia quella di sicurezza di prodotti e dispositivi concepita per beni fisici potenzialmente dannosi e nota come "*new legislative framework*"[479].
Si tratta di una disciplina calata maggiormente su prodotti e che meno si attaglia a sistemi di IA impiegati in ambito lavorativo ove i rischi concernono valori immateriali e diritti fondamentali dei lavoratori.
Da qui, derivano alcune criticità.

Il contenuto della regolamentazione, così come articolato e prospettato, può apparire insufficiente a garantire una tutela ai lavoratori.
In primo luogo, il richiamo al GDPR e ai principi dallo stesso sottesi può indurre delle difficoltà che non consentono l'effettiva applicazione della normativa richiamata.
Il GDPR, pur operando quale strumento generale per i diritti fondamentali in materia di protezione dei dati, sembra perseguire una prospettiva obsoleta nei confronti delle tecnologie emergenti, senza considerare le distinte modalità in cui possono essere impiegati i dati in forza delle nuove capacità algoritmiche di elaborazione[480].Il Regolamento adotta, infatti, un approccio volto a regolare la raccolta dei dati, ma trascura i rischi associati all'analisi degli stessi, facendo eccezione delle decisioni basate esclusivamente sul trattamento automatizzato, inclusa la profilazione.
Ciò determina l'esclusione degli effetti che un'analisi inferenziale può apportare, relativa a quelle elaborazioni che traggono conclusioni attraverso correlazioni o deduzioni logiche.
Il GDPR potrebbe, così, concentrarsi troppo sulla fase di *input*, al momento in cui i dati vengono raccolti, ma non abbastanza su come essi vengono valutati. Una volta acquisiti legittimamente, in ragione di una effettiva base giuridica, la loro elaborazione mediante analisi inferenziale rimarrebbe esente da ulteriori controlli[481].
Il modello offerto dal GDPR può, quindi, apparire difficilmente usufruibile dai lavoratori, altre che complesso nella sua applicazione (e burocratizzazione) da parte delle organizzazioni[482].
A mitigare tali *vulnus* potrebbero non risultare sufficiente il rimando a principi su cui si fonda la tutela dei dati personali quale il principio di minimizzazione.

---

mercato. Inoltre, spetta allo stesso *provider* condurre un sistema di gestione del rischio per mitigare i rischi tecnici che derivano dall'utilizzo del sistema.

479 Per *new legislative framework* si intende il nuovo quadro legislativo che mira a migliorare il mercato interno delle merci e a rafforzare le condizioni per l'immissione di un'ampia gamma di prodotti sul mercato dell'UE. Si tratta di un pacchetto di misure volte a migliorare la vigilanza del mercato e ad aumentare la qualità delle valutazioni di conformità.
Il quadro legislativo della disciplina è composto dal Regolamento (CE) 765/2008 che stabilisce i requisiti per l'accreditamento e la vigilanza del mercato dei prodotti; dal Regolamento (UE) 2019/1020 sulla vigilanza del mercato e sulla conformità dei prodotti e dalla Decisione 768/2008/CE del Parlamento europeo e del Consiglio che fornisce un quadro comune per la commercializzazione dei prodotti.

480 Cfr. Aloisi A., Gramano E., *Artificial intelligence is watching you at work: digital surveillance, employee monitoring, and regulatory issues in the Eu context,* in *Special Issue of Comparative Labor Law & Policy Journal, "Automation, Artificial Intelligence and Labour Protection",* edited by Valerio De Stefano, Vol. 41, n. 1, p. 127.

481 Cfr. Wachter S., Mittelstadt B., Russell C., *Counterfactual explanations without opening the black box: automated decisions and the GDPR,* in Harvard Journal of Law & Technology Vol. 31, n. 2 Spring 2018, pp. 861 ss.

482 In merito Zilli A., *La trasparenza nel lavoro subordinato. Principi e tecniche di tutela*, Pacini Giuridica, 2022, pp. 27 e ss.

Questo, infatti, appare potenzialmente eluso ogni qual volta i processi di elaborazione e correlazione dei dati, compiuti in modo automatico, siano in grado di ricavare altre informazioni che il titolare non avrebbe dovuto o voluto acquisire[483].
Parimenti, anche il principio di finalità del trattamento, definito *ex ante*, potrebbe venire meno qualora il sistema devi in maniera autonoma, durante il processo di elaborazione, dalle finalità preliminarmente dichiarate e accettate dall'utente.
Anche la tutela garantita dal principio di trasparenza e dal corrispondente diritto di informazione degli interessati a conoscere il funzionamento e la logica del sistema potrebbe trovare dei limiti in ragione dei vincoli posti dalla tutela dai segreti commerciali e dalla tutela del *know-how* (Direttiva (UE) 2016/943 sui cosiddetti "*trade secrets*").

Altre osservazioni critiche interessano il contenuto della proposta di Regolamento, più orientato a una logica di tutela del prodotto che a quella della persona.
La proposta di regolamento segue, infatti, un "*approccio regolamentare tradizionalmente utilizzato nella disciplina della sicurezza dei prodotti per garantire la tutela dei diritti fondamentali*", applicandolo anche a "*coloro che si interfacciano con la macchina intelligente*"[484].
L'AIR, dunque, identifica i soggetti che adoperano sistemi di IA quali "utenti" del sistema e, conseguentemente, inquadra il datore di lavoro che si avvale di tali strumenti quale "utilizzatore".
Questa prospettiva assimila il datore di lavoro ad un mero fruitore del sistema di IA, in quanto acquirente e utilizzatore di tali dispositivi.
In forza di ciò, il datore di lavoro sarà onerato da pochi obblighi in confronto a quelli imposti al fornitore, indicati prevalentemente nell'articolato dell'art. 29 della proposta di Regolamento, come quello di sospendere l'uso del sistema se presenti rischi per la salute e la sicurezza o minacci i diritti fondamentali degli interessati.
Da una tale logica, imperniata sulla garanzia del prodotto, discende una totale assenza di previsione di controlli o procedure di negoziazione rimesse alle Parti Sociali quando i sistemi di IA vengano impegnati nei rapporti di lavoro.
Si precisa, inoltre, che il Considerando 36 esclude il lavoratore quale "utente" ai fini dell'applicazione del Regolamento, generando un parziale *vulnus* normativo.
Se, infatti, i rischi in cui possono incorrere i lavoratori vengono espressamente considerati (includendo i sistemi di IA utilizzati nei contesti lavorativi tra quelli ad alto rischio), l'AIR omette di inserire i prestatori tra i soggetti destinatari di regole e, quindi, trascurando il loro *status* di titolari di specifici diritti[485].
Un'ulteriore critica che può essere mossa nei riguardi del AIR è la latenza di meccanismi di controllo e prevenzione per eventuali distorsioni nel funzionamento dei sistemi da cui possano pervenire *bias* e discriminazioni algoritmiche.
Opportunamente dovrebbero, quindi, trovare spazio i diritti collettivi a tutela dei lavoratori digitali, dato che l'emersione di nuovi rischi non può essere qualificata di rilevanza solo individuale.
Ciò non solo per garantire un'adeguata assistenza al singolo a una reale comprensione del funzionamento dei sistemi a cui è soggetto, ma anche per permettere un'effettiva trasparenza e accessibilità alla logica dei processi compiuti.

---

483 In merito Astone A., *Autodeterminazione nei dati e sistemi A.I.*, in *Contratto e impresa*, n. *2.*, 2022, pp. 429 ss.
484 Cappellazzo N., *L'art. 8 Stat. Lav. e i meccanismi di HR algorithms management: lo Statuto dei lavoratori alla prova delle nuove tecnologie*, in *Federalismi.it* del 9 agosto 2023, n. 21, p. 200.
485 In merito è stato osservato che AIR, a differenza del GDPR, non prevede "*strumenti di empowerment dei soggetti destinatari finali delle decisioni attuate tramite i sistemi automatizzati*". Abriani N., Schneider G., *Diritto delle imprese e intelligenza artificiale. Dalla Fintech alla Corptech*, il Mulino, Bologna, 2021, p. 118; Peruzzi M., *Intelligenza Artificiale e lavoro. Uno studio su poteri datoriali e tecniche di tutela,* Giappichelli Editore, Torino, 2023, pp. 69,70.

Se è vero, infatti, che i sistemi algoritmici e di IA ricadono nell'ambito di tutela della Direttiva "*trade secrets*", rimanendo soggetti ai limiti dalla stessa previsti, va anche ricordato che tale Direttiva all'art. 3[486] rende lecita l'acquisizione di un segreto commerciale se ottenuto nell'esercizio del diritto all'informazione e alla consultazione da parte dei rappresentanti dei lavoratori.

Il giudizio sulla proposta di Regolamento su IA non può essere, però, integralmente negativo.
In primo luogo, la centralità data al principio di trasparenza, da cui deriva un conseguente obbligo di informazione, determina il divieto di ogni strumento che non consenta un'effettiva conoscibilità dei sistemi di IA adoperati.
Per poter accedere a tali sistemi, dunque, il datore di lavoro deve garantirne la spiegabilità e, con essa, la conoscibilità delle logiche di funzionamento dei parametri.
L'impiego della tecnologia che opera in autonomia nell'ambito del diritto del lavoro deve fondarsi, pertanto, sul principio di trasparenza.
A riguardo ci si domanda, però, fino a che punto la conoscibilità e la trasparenza dei sistemi sia dovuta e se la valenza di tale principio sia un diritto individuale o se possa essere qualificato come collettivo, di cui ne possono essere portatrici le Parti Sociali o una rappresentanza dei lavoratori.
Il diritto all'intellegibilità e alla trasparenza è sistematizzato anche all'interno del *corpus* normativo del GDPR che introduce precisi obblighi informativi (agli artt. 13 e 14), nonché uno strumento giuridico diretto a disciplinare i processi decisionali automatizzati e dunque, di IA, sancendo un espresso diritto alla spiegazione e alla revisione umana (art. 22 GDPR).
Nel GDPR, però, il diritto è definito come una tutela individuale, delineando una dimensione personale delle prerogative dell'interessato.
Differentemente, nel Regolamento europeo sull'IA, quando si fa riferimento alla spiegabilità e alla trasparenza, queste vengano prospettate come un dovere che il datore di lavoro ha nei confronti della collettività dei lavoratori.
La previsione formula così come super individuale il diritto di informazione, ma non si pronuncia in favore di ulteriori poteri che consentano l'azione collettiva.

Il richiamo mosso dal AIR alla disciplina *privacy* acquisisce, inoltre, un'accezione positiva ove ci si rifaccia al principio di *accountability* e agli adempimenti che questa introduce.
La logica di responsabilizzazione e l'adozione di strumenti flessibili, adattabili secondo una logica "*tailor made*" alle peculiari esigenze di ogni realtà lavorativa, è un elemento di forza, introducendo un approccio adatto a fronteggiare il celere sviluppo della tecnologia e le conseguenze derivanti dal mutamento.

Ulteriore elemento a cui viene data attenzione nella proposta di Regolamento IA è il principio di proporzionalità, intrinsecamente connesso ai principi di equità e minimizzazione.
Il principio di proporzionalità appare direttamente legato alla responsabilità del datore di lavoro e, quindi, alla logica di *accountability* e di gestione del rischio. Si tratta di un approccio basato sulla valutazione dell'entità del rischio e sulle potenzialità dannose che possono scaturire dai sistemi tecnologici adottati.

---

[486] Direttiva (UE) 2016/943, art. 3 "*Acquisizione, utilizzo e divulgazione leciti dei segreti commerciali 1. L'acquisizione di un segreto commerciale è considerata lecita qualora il segreto commerciale sia ottenuto con una delle seguenti modalità: a) scoperta o creazione indipendente; b) osservazione, studio, smontaggio o prova di un prodotto o di un oggetto messo a disposizione del pubblico o lecitamente in possesso del soggetto che acquisisce le informazioni, il quale è libero da qualsiasi obbligo giuridicamente valido di imporre restrizioni all'acquisizione del segreto commerciale; c) esercizio del diritto all'informazione e alla consultazione da parte di lavoratori o rappresentanti dei lavoratori, in conformità del diritto e delle prassi dell'Unione e nazionali; d) qualsiasi altra pratica che, secondo le circostanze, è conforme a leali pratiche commerciali. 2. L'acquisizione, l'utilizzo o la divulgazione di un segreto commerciale sono da considerarsi leciti nella misura in cui siano richiesti o autorizzati dal diritto dell'Unione o dal diritto nazionale*".

Questo impone al datore di lavoro, in quanto responsabile dell'organizzazione, una serie di obblighi al fine di garantire l'affidabilità di tali sistemi.
La logica adottata dalla proposta di Regolamento europeo sulla IA, imperniata su un approccio *risk based*, fa sorgere una presunzione legale di "alto rischio" in corrispondenza dell'applicazione di sistemi automatici e di IA nell'ambito del lavoro.
L'utilizzo di tali sistemi è, quindi, posto ad un alto livello di attenzione e qualsiasi applicazione in ambito lavorativo richiede l'adozione di cautele specifiche, soprattutto ove ne possa scaturire un controllo dei lavoratori.
La proposta di Regolamento su IA fornisce a riguardo un'indicazione dei possibili modelli di gestione, ma limita la tutela anticipandola all'introduzione dei sistemi e concentrandosi sugli obblighi che ricadono in capo al produttore e non su chi li utilizza, ovvero il datore di lavoro.

Ulteriore principio a cui fa riferimento la proposta di Regolamento è quello personalista, da cui discende un approccio antropocentrico e un corrispondente diritto a ricevere una sorveglianza umana. Il Regolamento rigetta, in tal modo, un'operatività integralmente autonoma dei sistemi algoritmici le cui implicazioni saranno di seguito analizzate al punto 3.4.

3.2. La proposta di Direttiva sul lavoro mediante piattaforme

L'articolato della proposta di Direttiva sul lavoro mediante piattaforme[487] recepisce e sviluppa i principi posti a fondamento del nuovo pacchetto regolativo europeo in materia di lavoro digitale e impiego di sistemi algoritmici.
In primo luogo, fa riferimento al principio di responsabilità e affidabilità del datore di lavoro.
Le piattaforme digitali adoperate nei rapporti di lavoro sono strumenti ad "alto rischio", secondo la definizione fornita dalla proposta di Regolamento su IA (Considerando 36 AIR).
Se, dunque, l'uso di tali strumenti comporta un "alto rischio" per i lavoratori, di conseguenza risulta essenziale introdurre una regolamentazione volta a prevenire e contrastare i pericoli che possono coinvolgere i prestatori digitali.
Un secondo principio sostanziale a cui fa riferimento è quello della trasparenza e spiegabilità dei sistemi algoritmici e di IA impiegati, prevedendo che siano decifrabili e intellegibili.
La proposta di Direttiva predispone a riguardo un assetto di regole specifiche a seconda che i sistemi automatizzati siano decisionali o di monitoraggio; norme contenute nel capo terzo dedicato alla "*gestione algoritmica dei lavoratori*".

---

[487] In merito si rinvia a Donini A, *Piattaforme*, in Novella M., Tullini P. (a cura di), *Lavoro digitale*, Giappichelli Editore, 2022, pp. 25-45; Delfino M., *Lavoro mediante piattaforme digitali, dialogo sociale europeo e partecipazione sindacale*, in *Federaslismi.it*, n. 25, 2023, pp. 170 ss; Purificato I., Senatori I., *The Position of Collective Rights in the 'Platform Work' Directive Proposal: Commission v Parliament*, in *Hungarian Labour Law E-Journal*, n. 1, 2023, pp. 1 ss; Otto M., *A step towards digital self- & co-determination in the context of algorithmic management systems*, in *Italian Labour Law e-Journal*, 2022, 2, p. 51 ss; Spinelli C., *La trasparenza delle decisioni algoritmiche nella proposta di Direttiva UE sul lavoro tramite piattaforma*, in *Lavoro Diritti Europa*, n. 2, pp. 6 ss; Tebano L., *La digitalizzazione del lavoro tra intelligenza artificiale e gestione algoritmic*a; in *IANUS*, n. 24, 2021, pp. 42 ss; Tebano L, *Fabbrica 4.0 e potere di "controllo direttivo"*, in Rusciano M., Gaeta L., Zoppoli L. (a cura di), *Mezzo secolo dallo statuto dei lavoratori*, in *Quaderni della Rivista Diritti Lavori Mercanti,* n. 8, 2020, pp. 443 ss.; Treu T., *La digitalizzazione del lavoro: proposte europee e piste di ricerca*, in *Federalismi.it,* n. 9, 2022, p. 190 ss.; Alaimo A., *Il pacchetto di misure sul lavoro nelle piattaforme: dalla proposta di Direttiva al progetto di Risoluzione del Parlamento europeo. Verso un incremento delle tutele*?, in *Labour & Law Issues (LLI),* vol. 8, n. 1, 2022, R.1- R.28; Alaimo A., *Lavoro e piattaforme tra subordinazione e autonomia: la modulazione delle tutele nella proposta della Commissione europea*, in *Diritto delle Relazioni Industriali*, n. 2, 2022, pp.639 ss.; Abraha H., Adams-Prassl J., Kelly Lyth A., *Finetuning the EU's Platform Work Directive*, in *Oxford Business Law Blog*, del 17 maggio 2022, disponibile al *link* https://blogs.law.ox.ac.uk/business-law-blog/blog/2022/05/finetuning-eus-platform-work-directive; Barbieri M., *Prime osservazioni sulla proposta di direttiva per il miglioramento delle condizioni di lavoro nel lavoro con piattaforma*, in *Labour & Law Issues (LLI),* vol. 7, n. 2, 2022, C1-C.20.

La proposta di Direttiva riconosce, quindi, il diritto alla trasparenza in merito all'uso e al funzionamento dei sistemi automatizzati adoperati per assumere decisioni che incidano significativamente sulle condizioni di lavoro (art. 6 proposta di Direttiva).
La proposta di Direttiva promuove, infine, una logica antropocentrica prevedendo un monitoraggio dell'impatto che questi sistemi possono avere sui soggetti interessati e garantendo un riesame umano delle decisioni che incidono in maniera significativa sulle condizioni dei lavoratori. La normativa consente, così, ai prestatori di rivolgersi a una persona di contatto competente, designata dalla piattaforma, per discutere e chiarire le circostanze delle disposizioni assunte (artt. 6, 7, 8 della proposta di Direttiva).
Tale approccio determina tre conseguenze: la revisione umana risulta necessaria ogni qualvolta vengano prese decisioni automatizzate, che tale revisione si attiva su *input* della persona interessata e che le decisioni assunte devono risultare significative[488].

Nonostante la normativa si fondi su tali principi guida, permangono alcuni profili di criticità che riecheggiano quelli riscontrati nel testo della proposta di Regolamento su IA.
Il primo interessa il livello di trasparenza a cui si deve rispondere per il legittimo utilizzo dei sistemi di gestione algoritmica dei lavoratori. Ci si chiede in merito quanto sia realmente accessibile un sistema algoritmico e quanto delle informazioni condivise con i singoli lavoratori risulti comprensibile.

In secondo luogo, la proposta di Direttiva prevede (ancora) una interlocuzione tra il singolo lavoratore e la piattaforma digitale. Il principio di trasparenza è, infatti, costruito come un diritto individuale, al pari di quanto previsto dal GDPR all'art. 22, riconoscendo solo un ambito circoscritto al soggetto collettivo[489].
Si ravvisa, infatti, ancora una volta l'assenza di un modello di vera e propria regolamentazione collettiva ritrovando, negli articoli 6 e 9 della proposta, uno schema meramente "informativo"[490] nei confronti delle Parti Sociali.
Scelta che sarebbe forse più adatta a far fronte a situazioni dinamiche come quelle proposte dall'innovazione digitale, potendo garantire l'equilibrio tra le innovazioni organizzative e le esigenze di flessibilità.
Meccanismo che già esiste a livello europeo e lo si ritrova proposto all'interno dell'Accordo quadro europeo di digitalizzazione del giugno 2020 in cui si propongono schemi di consultazione dei rappresentanti dei lavoratori per l'analisi preventiva e *in fieri* dell'assetto digitale aziendale. Lo stesso Accordo prevede, inoltre, un sistema di verifiche e indagini *ex post* al fine di una eventuale ridefinizione degli assetti contrattuali aziendali così da indicare le protezioni maggiormente attinenti alle esigenze riscontrate.

Il terzo aspetto critico riguarda il diritto alla sorveglianza umana, ovvero il diritto delle persone a non essere gestite e giudicate esclusivamente da una macchina.
La proposta di Direttiva prevede che qualora il lavoratore non sia soddisfatto dell'utilizzo della piattaforma, ossia di come venga valutato dalla stessa, possa richiedere un riesame umano per le decisioni automatizzate che incidano significativamente sulle sue condizioni di lavoro.

---

488 Cfr. Abraha H., Adams-Prassl J., Kelly Lyth A., *Finetuning the EU's Platform Work Directive*, in *Oxford Business Law Blog*, del 17 maggio 2022.
489 In merito si rinvia a Purificato I., Senatori I., *The Position of Collective Rights in the "Platform Work" Directive Proposal: Commission v Parliament*, in *Hungarian Labour Law E- Journal*, 2023/1, consultabile sul sito http://www.hllj.hu.
490 La medesima impostazione è stata riproposta anche da Decreto Trasparenza tanto da postare alcuni primi commentatori a definire come meramente di cammeo il ruolo ricoperto dal sindacato. Cfr. Faioli M., *Trasparenza e monitoraggio digitale. Perché abbiamo smesso di capire la norma sociale europea*, in *Federalismi.it*, del 5 ottobre 2022, n. 25, pp. 104 – 115.

Previsione analoga a quella contenuta nell'art. 22 del GDPR che riconosce agli interessati il diritto di ricevere una decisione umana quando sono coinvolti processi di elaborazione automatizzata dei dati che producano effetti giuridici o incidano in modo significativo su di essi[491].
Si tratta di un diritto esercitabile solo *ex post*, ovvero quando la decisione è stata assunta. Si tratta, inoltre, di un riesame umano che deve fornire una motivazione alla decisione automatica assunta, ma che non è soggetta ad alcun controllo esplicito o a forme di contestazione.
Un riesame delle decisioni *ex post* potrebbe, dunque, non essere sufficiente per comprendere a pieno le logiche dell'algoritmo che, per essere accessibile, potrebbe necessitare di procedure preventive e *in itinere* che accompagnino il processo decisionale.
Previsione, quella di un controllo *ex ante* e *in itinere*, presente nelle precedenti versioni della proposta di Direttiva, ma espunta da quella attuale affievolendo, in tal modo, il principio personalista e il diritto a ricevere una sorveglianza umana.

L'approccio cosiddetto *human on command*[492] si sostanzia, inoltre, nella possibilità dei soggetti interessati ad ottenere delle spiegazioni e risulta direttamente connesso al diritto di impugnare la decisione algoritmica e di ottenerne un riesame umano che tenga conto delle prospettive dei singoli interlocutori.
Il diritto di esprimere la propria opinione è, dunque, parte integrante della tutela.
Tale facoltà risulta, però, attualmente assente dal dettato dell'art. 8 della proposta di Direttiva, a differenza di quanto previsto espressamente dall'art. 22 paragrafo 3 del GDPR il quale prevede che "*il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione".*
L'assenza di un riferimento al diritto di esprimere una propria opinione dovrebbe, quindi, trovare esplicita integrazione nell'emanando dettato normativo al fine di salvaguardare, da un lato, la dignità umana e il diritto all'autodeterminazione dei lavoratori – favorendone la partecipazione- e, dall'altro, di incrementare la probabilità di ottenere decisioni corrette in quanto fondate su informazioni esaustive e pertinenti fornite dai diretti interessati[493]
Vi è, infine, un problema (comune) di sovrapposizione tra disposizioni che regolano la gestione algoritmica con quelle contenute nella proposta del Regolamento europeo sull'IA e con l'articolo 1bis introdotto dal Decreto Trasparenza, con evidenti difficoltà di coordinamento delle diverse discipline con riguardo al loro campo di applicazione a partire dalla stessa nozione di piattaforma digitale e agli adempimenti pratici a cui è tenuto il datore di lavoro.

La valutazione della proposta di Direttiva non può essere, però, integralmente negativa.

---

491 Art. 22 par. 3 del GDPR "*Nei casi di cui al paragrafo 2, lettere a) e c), il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione*".

492 Cfr. Parere del 31 maggio 2017 del Comitato economico e sociale europeo su "*L'intelligenza artificiale — Le ricadute dell'intelligenza artificiale sul mercato unico (digitale), sulla produzione, sul consumo, sull'occupazione e sulla società*" (2017/C 288/01), relatrice Catelijne Muller. Al punto 1.6 di pagina 2 si legge che "*Il CESE raccomanda di adottare, nei confronti dell'IA, l'approccio «human-in-command», con la condizione essenziale che l'IA sia sviluppata in maniera responsabile, sicura e utile, e che la macchina rimanga macchina e l'uomo ne mantenga il controllo in ogni momento".* In merito anche *International Labour Organization* (ILO), *Global Commission on the future work,* nel documento"*Work for a bright future*" del 2 luglio 2019.

493 Sul punto il commento di Marta Otto la quale sostiene che "*the ratio legis of the explicit introduction of the right to express one's own position boils down, on the one hand, to safeguard respect for human dignity and the right to self-determination by allowing active participation; and, on the other hand, to increase the likelihood of correct decisions based on complete information obtained by filling in missing and relevant information through the direct participation of data subjects*". Otto M., *A step towards digital self-& co-determination in the context of algorithmic management systems*, in *Italian Labour Law e-Journal*, n. 1, vol. 15, 2022, p. 59.

Con essa, infatti, il Parlamento Europeo promuove la contrattazione collettiva, riconoscendo un diritto all'informazione ai lavoratori e ai loro rappresentanti.
Diritto che acquisisce, quindi, un'accezione ampia proponendosi di garantire non solo la trasparenza dei sistemi ai singoli lavoratori, ma favorendo – contestualmente - nuove forme partecipative e nuovi diritti collettivi che permettano di superare le opacità presenti nel funzionamento delle strutture delle piattaforme digitali[494].
Il coinvolgimento dei rappresentanti dei lavoratori nelle varie fasi di funzionamento dei sistemi automatizzati potrebbe non solo intervenire sull'esercizio del potere datoriale, ma potrebbe anche contribuire a limitare - se non rimuovere - le asimmetrie informative, contribuendo a realizzare una gestione trasparente ed equa dei sistemi algoritmici.
Con la proposta di Direttiva si introduce, così, una dimensione superindividuale del principio di trasparenza, riconoscendo una forza collettiva ai diritti di informazione al fine di rafforzare la centralità del controllo umano sui meccanismi adottati dai sistemi algoritmici.

4. Principio di trasparenza quale funzione abilitante dei diritti dei lavoratori

La ricostruzione svolta nel presente studio mostra come i dati tendono a presentarsi secondo una duplice prospettiva: come diritto della persona del lavoratore, ma anche come un bene connotato da un valore economico e sociale per la realizzazione di interessi datoriali e non solo.
La ricerca compiuta rivela, inoltre, come i dati giungano ad un livello di interconnessione tale per cui è sempre più difficile attribuire ad essi a priori un valore certo e univoco**.**
Lo stato dell'arte non permette più di definire i dati esclusivamente in una dimensione personalistica, escludendo le potenzialità intrinseche a tali elementi che possono essere sfruttate in quanto strumenti innovativi per trarre decisioni più efficaci.

Vi è, dunque, una maturazione sulla politica dei dati che superando un pregresso atteggiamento esclusivamente difensivo[495], volto a tutelare la *privacy* degli interessati[496] e di "autodeterminazione informativa"[497], induce a considerare una gestione che apra verso uno sfruttamento condivisibile delle loro potenzialità.
"*Il dato viene considerato in positivo come risorsa, nella sua qualità di generatore di valore, e non più solo come bene staticamente da preservare e custodire*"[498].

494 Cfr. Purificato I., Senatori I., *The Position of Collective Rights in the "Platform Work" Directive Proposal: Commission v Parliament*, in *Hungarian Labour Law E- Journal*, 2023/1, consultabile sul sito http://www.hllj.hu; Ales E., Bel M., Deinert O., Robin-Olivier S. (a cura di), *International and European Labour Law: Article-by-Article Commentary,* London, Beck Hart Nomos, 2018, pp. 214–218 sull'articolo 27 CFUE "*Diritto dei lavoratori all'informazione e alla consultazione all'interno dell'impresa*".
495 Da intendersi quale diritto alla protezione dei dati personali e a un corrispettivo controllo dei trattamenti sugli stessi compiuti. In merito Scagliarini S., *La tutela della privacy e dell'identità personale nel quadro dell'evoluzione tecnologica,* in *Consulta OnLine*, n. 2, 2021, pp. 489 ss.; Gambino A.M., Stazi A. (a cura di), *La circolazione dei dati. Titolarità, strumenti negoziali, diritti e tutele,* Pacini Giuridica, Pisa, 2020.
496 Il diritto alla riservatezza che, secondo la Corte costituzionale trova riferimento nella Costituzione italiana negli articoli 2,14 e 15 e che incontra specifica protezione nelle varie norme europee e convenzionali, si caratterizza oggi "*particolarmente quale diritto a controllare la circolazione delle informazioni riferite alla propria persona*". Sentenza delle Corte costituzionale del 23 gennaio 2019, n. 20. Per un commento Nicotra I., *Privacy vs trasparenza, il Parlamento tace e il punto di equilibrio lo trova la Corte*, in *Federalismi.it*, n. 7, 2019, pp. 1 ss.; Scagliarini S., *La tutela della privacy e dell'identità personale nel quadro dell'evoluzione tecnologica,* in *Consulta OnLine*, n. 2, 2021, pp. 599 ss.
497 Scagliarini S., *La tutela della privacy e dell'identità personale nel quadro dell'evoluzione tecnologica,* in *Consulta OnLine*, n. 2, 2021, p. 569.
498 Trojsi A*, Sull'impatto giuslavoristico del Data Governance Act. Riflessioni sistemiche a prima lettura del Regolamento (UE) 2022/868*, in *Federalismi.it*, n. 4, 2022, p. 283.

In tale prospettiva si sviluppa il Regolamento europeo 2022/868 sulla *governance* dei dati (DGA)[499], applicabile dal 24.09.2023, in cui il dato è considerato come risorsa e generatore di valore, non più solo come bene da preservare e custodire staticamente[500].
Il DGA introduce, infatti, il concetto di "governo dei dati" promuovendo una disciplina che regoli la circolazione, la condivisione e il riutilizzo, all'interno dell'Unione, di determinate categorie di dati[501].
L'obiettivo del DGA è bilanciare la tutela della concorrenza al fine di favorire una sempre più libera circolazione dei dati promuovendo la cosiddetta "*data economy*"[502], ovvero l'economia incentrata sui dati, sulle tecniche di raccolta, sull'elaborazione e condivisione[503] degli stessi.
Il fine del DGA è, dunque, quello di "*rendere disponibili più dati e a facilitare la condivisione dei dati tra i settori e i paesi dell'UE al fine di sfruttare il potenziale dei dati a vantaggio dei cittadini e delle imprese europei*"[504], nonché "*creare fiducia tra gli individui e le imprese per quanto riguarda l'accesso ai dati, la loro condivisione e il loro controllo, utilizzo e riutilizzo, in particolare stabilendo adeguati meccanismi per gli interessati affinché conoscano ed esercitino fattivamente i propri diritti*" (Considerando 5).
I dati (personali e non) vengono, quindi, considerati quali "risorsa economica" in quanto strumenti posti nella disponibilità di imprese - pubbliche e private - dal cui utilizzo è possibile trarre decisioni che meglio si adattano alle singole necessità.
Il DGA si pone, così, all'interno della "*Strategia europea per i dati*"[505] attuata dall'Unione Europea mediante l'operato della Commissione Europea e sviluppata su tre pilastri[506].
Il primo inerisce l'attuazione di un quadro legislativo abilitante per la *governance* dei dati. Il secondo, auspica la creazione di infrastrutture per la condivisione dei dati e di intelligenza artificiale. Il terzo pilastro, infine, mira a ingenerare fiducia nei meccanismi di riutilizzo dei dati, fornendo idonee tutele ai soggetti coinvolti e investendo sulla competenza.

---

499 Per un approfondimento sul DGA e sul suo impatto in ambito giuslavoristico si rinvia al lavoro di Trojsi A*, Sull'impatto giuslavoristico del Data Governance Act. Riflessioni sistemiche a prima lettura del Regolamento (UE) 2022/868*, in *Federalismi.it*, n. 4, 2022, pp. 276 ss; Spinelli C., *Il regolamento (UE) 2022/868 sulla governance dei dati e le sue possibili ricadute sulle misure di inclusione lavorativa delle persone con disabilità*, in *Federalismi.it*, n. 9, 2023, pp. 257 ss.

500 Il DGA sarà, inoltre, ulteriormente integrato dalla proposta di Regolamento del 23 febbraio 2022 (Data Act) che detta regole armonizzate per il corretto accesso e uso dei dati (personali e non) generati dall'uso dei prodotti connessi e dei servizi correlati, al fine di garantire un'equità dei contratti di condivisione dei dati. A riguardo il 14 marzo 2023 sono stati approvati gli emendamenti del Parlamento europeo apportati alla proposta di Regolamento riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo. Il testo può essere consultato al seguente *link*:https://www.europarl.europa.eu/doceo/document/TA-9-2023-0069_IT.pd

501 Per "dati" il regolamento intende "*qualsiasi rappresentazione digitale di atti, fatti o informazioni e qualsiasi raccolta di tali atti, fatti o informazioni, anche sotto forma di registrazione sonora, visiva o audiovisiva*" Art. 2 punto 1. Il Regolamento si riferisce, quindi, sia ai dati personali a cui fa riferimento il GDPR, sia quelli "non personali", intesi come tutti i dati non personali ossia anonimi.

502 Termine impiegato nel DGA, ove si fa riferimento a una "*economia basata sui dati inclusiva*" (Considerando 2 DGA), nonché anche nel *European Data Market study* che ha il fine di monitorare il mercato europeo dei dati e fornire informazioni essenziali alla Commissione europea sulle dimensioni e sulle tendenze del mercato dei dati, nonché sull'economia dati dell'UE, sul numero di professionisti dei dati, sul numero di società di dati e sui ricavi da loro creati. Fonte sito dell'Unione Europea consultabile al *link* https://digital-strategy.ec.europa.eu/en/library/results-new-european-data-market-study-2021-2023.

503 In riferimento ai meccanismi aperti e collaborativi di condivisione dei dati si rinvia a Poletti D., *Gli intermediari dei dati*, in *European Journal of Privacy Law & Technologies*, n. 1, 2022, pp. 45 ss.

504 Sito dell'Unione europea "*Plasmare il futuro digitale dell'Europa*" consultabile al *link* https://digital-strategy.ec.europa.eu/it/policies/data-governance-act.

505 Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni "*Una strategia europea per i dati*" (COM(2020) 66 final del 19 febbraio 2020).

506 Finalità presenti nella comunicazione del 19 febbraio 2020 della Commissione europea "strategia europea per i dati" ove viene descritta la visione uno spazio comune europeo di dati: "*un mercato interno dei dati nel quale questi ultimi possano essere utilizzati indipendentemente dal loro luogo fisico di conservazione nell'Unione, nel rispetto della normativa applicabile, che tra le altre cose potrebbe essere centrale per il rapido sviluppo delle tecnologie di intelligenza artificiale*" (Considerando 2 DGA).

L'obiettivo dell'Unione europea appare, dunque, chiaro e si concretizza nella volontà di generare valore dai dati attraverso il loro utilizzo mediante un incremento della loro circolazione e condivisione attraverso l'aumento della fiducia negli intermediari dei dati.

Tale impostazione pone un problema di regolamentazione nei riguardi dell'utilizzo dei dati indicati quali principali fattori di innovazione per il mondo del lavoro.
Ciò non significa, però, rinnegare le conquiste ottenute in materia di protezione dei dati personali e di tutele dei lavoratori.
Il nuovo corso valorizzante dei dati è possibile proprio in forza dell'apparato normativo di tutela previsto su cui innestarsi quale imprescindibile presupposto[507].
Vi è, quindi, la necessità di uno sfruttamento dei dati che sia regolato sulla base di norme che ingenerino fiducia nei lavoratori e ne preservino i diritti.
I dati acquisiti non devono, pertanto, essere solo accessibili, ma avere caratteristiche di qualità ovvero essere selezionati per lo scopo prefissato e sicuri in ragione al loro utilizzo.
Tali criticità e potenzialità devono essere sfruttate per elaborare politiche del lavoro aderenti alla realtà e che consentano di formulare regole calibrate sulle esigenze emergenti dalla datificazione del lavoro.

In forza di tali premesse, il diritto del lavoro, proprio perché parte dell'elemento organizzativo, ricopre la funzione di tutela evolutiva, adattandosi alla tecnologia che si innova.
Il fine è certo, ovvero quello di tutelare la dignità e riservatezza dei lavoratori, ma i mezzi per raggiungerlo devono adattarsi al contesto.

Per tale ragione occorre (ri)definire il concetto di controllo a distanza dei lavoratori e i suoi limiti, interrogandosi su quando nasca l'effettiva manifestazione di tale potere.
L'incertezza nella definizione di cosa costituisca "controllo" e del momento in cui esso può essere esercitato determina un'opacità nella manifestazione del potere e una vulnerabilità delle posizioni di tutela dei prestatori.
Il cuore del problema porta, dunque, a riflettere su come si definiscano i limiti dei poteri datoriali in un contesto algoritmico.

Se si parla di limiti al potere di controllo, il patrimonio normativo nazionale impone di prendere in esame la funzione limitativa attuata dall'art. 4 SL e dall'autonomia collettiva.
In tale ambito l'art. 4 SL, con la distinzione tra strumenti di lavoro e di controllo, non appare più soddisfacente, presupponendo un sistema rigido capace di distinguere i diversi strumenti. Classificazione che si rivela anacronistica e mostra i propri limiti dinanzi alla natura polifunzionale dei dispositivi digitali e alla dematerializzazione del luogo di lavoro.
Parimenti, anche la richiesta di intervento delle rappresentanze dei lavoratori ai fini dell'installazione degli strumenti di controllo diviene limitata in forza della parzialità delle informazioni che vengono condivise in tale contesto.

[507] Il rapporto tra DGA e GDPR è esplicato dallo stesso Regolamento europeo 2022/868 all'art. 1 secondo cui il diritto dell'unione nazionale in tema di protezione dei dati si applica a qualsiasi dato personale trattato e non pregiudica i poteri del GDPR anche in relazione alle competenze delle autorità di controllo. Il diritto dell'unione nazionale della protezione dati personali prevale in caso di conflitto con il DGA. Il DGA non crea, infine, una base di trattamento dei dati personali e non influisce sui diritti obblighi del GDPR. Il problema del nesso con il GDPR viene superato nel momento in cui dell'utilizzo di processi tecnologici i dati vengono spersonalizzati mediante anonimizzazione o pseudo anonimizzazione come pure cifratura dei dati. Viceversa, viene di nuovo in campo il GDPR in caso di deanonimizzazione dei dati originariamente cifrati.

Il limite posto dalla valutazione esclusivamente preliminare in merito all'opportunità di installare uno strumento di controllo risulta scarso, non potendo soddisfare la condizione di conoscibilità delle informazioni accessibili, anche solo potenzialmente, mediante l'elaborazione tecnologica.

Il tema del potere di controllo algoritmico e dei suoi limiti si interseca, quindi, strettamente con quello della trasparenza e del diritto di informazione.
L'utilizzo di sistemi di elaborazione algoritmici o basati su IA, non comprensibili per chi sia privo di competenze specifiche di carattere tecnico-informatico, è una delle cause che generano un incremento sproporzionato dei poteri datoriali e un conseguente squilibrio tra le parti del rapporto di lavoro.

Ove la manifestazione dei poteri datoriali divenga incerta e opaca, si rivela necessaria la costruzione di azioni di contenimento che proteggano la dignità e la riservatezza del lavoratore in un contesto fortemente modificato dall'innovazione digitale.
Il Legislatore europeo muove da questa consapevolezza, conscio che le asimmetrie informative costituiscano un'alterazione del rapporto di lavoro capaci di generare espressioni di potere datoriale.
Il ruolo, quindi, che le norme europee attribuiscono ai diritti di informazione è quello di compensazione di una deprivazione informativa che deriva dalla potenzialità delle nuove tecnologie.
Gli obblighi di informazione vengono richiamati in differenti ambiti a partire dal testo del GDPR che, negli articoli 13 e 14, prevede specifici oneri in capo al titolare del trattamento, tra cui quello di comunicare la logica dei sistemi automatizzati.
Altri obblighi di informazione si rinvengono nella proposta di Direttiva sulle piattaforme digitali ove all'art. 9 si formula un diritto di informazione in due livelli garantito, in *primis,* ai rappresentanti dei lavoratori e, in mancanza, ai singoli lavoratori delle piattaforme digitali.
Il Legislatore europeo muove da un'esigenza di informazione che deve essere facilmente comprensibile e che deve essere formulata in maniera concisa, trasparente e intellegibile, nonché deve essere facilmente accessibile mediante un linguaggio chiaro e semplice (art. 6 della Proposta di Direttiva sulle piattaforme).

Il diritto di informazione è accompagnato e rafforzato da ulteriori tutele, come quella di ottenere una spiegazione per qualsiasi decisione presa o sostenuta dal sistema algoritmico, di poterne richiedere il riesame (art. 8 Proposta di Direttiva sulle piattaforme) e di opporsi a decisioni completamente automatizzate (art. 22 GDPR).

L'obbligo di informazione non si limita, quindi, ad assolvere una funzione esclusivamente comunicativa del linguaggio o della logica della macchina, ma è finalizzato a istruire il lavoratore affinché sia posto nella condizione di poter assumere decisioni consapevoli e responsabili.
La trasparenza di informazione riveste, pertanto, una funzione abilitante dei diritti del lavoratore nella sua duplice dimensione: quella interna di "tracciabilità" del processo decisionale e in quella "esterna" intesa come "spiegabiltà"[508] del medesimo.

[508] In merito alla dimensione "esterna" del principio di trasparenza, la Commissione europea nella comunicazione "*Creare fiducia nell'intelligenza artificiale antropocentrica*" del 8 aprile 2019 destinata al Parlamento europeo, al Consiglio, al Comitato economico e al Comitato delle regioni sottolinea l'esigenza che "*dovrebbero anche essere disponibili spiegazioni sulla misura in cui un sistema di IA influenza e definisce il processo decisionale organizzativo, le scelte di progettazione del sistema e la logica alla base della sua diffusione, in modo da garantire la trasparenza non solo dei dati e dei sistemi, ma anche dei modelli di business*" COM(2019) 168 final, p. 6.
In riferimento al principio di trasparenza come diritto a ricevere una spiegazione delle decisioni algoritmiche la giurisprudenza ammnistrativa nazionale ha enucleato "*gli elementi di minima garanzia per ogni ipotesi di utilizzo di algoritmi in sede decisoria pubblica: a) la piena conoscibilità a monte del modulo utilizzato e dei criteri applicati; b) l'imputabilità della decisione all'organo titolare del potere, il quale deve poter svolgere la necessaria verifica di logicità e legittimità della scelta e degli esiti affidati all'algoritmo*" (Consiglio di Stato, sezione VI,

In tal senso si è mosso anche il Legislatore italiano con il Decreto Trasparenza del giugno 2022, configurando un diritto del lavoratore a essere sempre informato riguardo l'utilizzo di sistemi di monitoraggio e decisionali automatizzati[509].

Se, dunque, la trasparenza dei sistemi è la garanzia posta a controbilanciare l'esercizio arbitrario del potere datoriale di controllo, in che termini devono prospettarsi i diritti di informazione di "nuova generazione"?

4.1. Applicazione del principio di trasparenza per la creazione di diritti di informazione più strutturati capaci di indagare non solo sugli strumenti impiegati

In primo luogo, i diritti di informazione di "nuova generazione" devono risultare più strutturati rispetto alla mera richiesta di autorizzazione all'installazione a cui fa riferimento l'art. 4 SL.

L'impiego di dati, in particolare ove "non autoevidenti", può comportare un cambiamento di paradigma nell'osservazione e nel controllo dei lavoratori basato sul criterio di correlazione.

Ciò può determinare una difficoltà nel garantire una spiegazione alle decisioni assunte dagli algoritmi.

Il diritto di informazione e la conseguente accessibilità alle caratteristiche del processo decisionale dovrebbe consentire ai lavoratori di comprendere non solo i risultati ottenuti, ma anche il modello impiegato dal sistema algoritmico.

L'autorizzazione all'installazione diviene un momento di tutela che appare perciò limitato, non essendo in grado di garantire i lavoratori di fronte alle capacità di elaborazione degli algoritmi e di acquisizione di nuove informazioni.

Il rispetto del principio di trasparenza deve, invece, essa essere capace di garantire non solo la comunicabilità, ma anche l'intellegibilità del sistema[510].

La protezione del lavoratore verrebbe, dunque, garantita "*svelando l'algoritmo, che dovrebbe divenire, in qualche modo, conoscibile, criticabile e, quindi, negoziabile*"[511].

La salvaguardia della trasparenza trova ulteriore sviluppo in un'interpretazione più incisiva delle proprie potenzialità, ultronee alla mera comprensione della logica sottesa al funzionamento dell'algoritmo.

Secondo tale declinazione del principio, la trasparenza può essere intesa come *"l'ostensione degli elementi considerati dal datore, al fine di ogni suo processo decisionale: l'indagine non si svolge sul quomodo (cioè sugli strumenti usati per decidere, che, spesso, come detto, sfuggono a tutti i soggetti coinvolti) ma sui presupposti (input) e sugli esiti (output)*"[512].

Una tutela della trasparenza basata esclusivamente sull'analisi degli strumenti e sul loro funzionamento appare, dunque, parziale, non tenendo conto degli elementi centrali dell'elaborazione (ossia i dati) e del loro potenziale informativo.

Sulla base di tali riflessioni, le nuove norme di legislazione europea si pongono l'obiettivo di implementare l'accessibilità e la conoscibilità delle informazioni oggetto di elaborazioni algoritmiche.

---

sentenza del 13 dicembre 2019, n. 8472, punto 12). In merito Lo Sapio G., *La trasparenza sul banco di prova dei modelli algoritmici,* in *Federalismi.it*, n. 11, 2021, pp. 238 ss.

509 In merito, anche nella Direttiva 2019/1152 del 20 giugno 2019 in materia di trasparenza e prevedibilità delle condizioni contrattuali il Legislatore europeo si era mosso configurando il diritto di informazione come strumento di tutela dei lavoratori.

510 In merito si è anche fatto riferimento al principio di trasparenza come "diritto alla conoscibilità delle procedure" e a un conseguente "principio di trasparenza algoritmica". Cfr. Covelli R., *Lavoro e intelligenza artificiale: dai principi di trasparenza algoritmica al diritto alla conoscibilità*, in *Labour & Law Issues (LLI),* vol. 9, n. 1, 2023, pp. I 77 ss.

511 Zilli A., *La trasparenza nel lavoro subordinato. Principi e tecniche di tutela*, Pacini Giuridica, 2022, p. 66, Libro in Open Access scaricabile gratuitamente dall'archivio IRIS – Anagrafe della ricerca https://air.uniud.it/.

512 Zilli A., *La trasparenza nel lavoro subordinato. Principi e tecniche di tutela*, Pacini Giuridica, 2022, p. 67, Libro in Open Access scaricabile gratuitamente dall'archivio IRIS – Anagrafe della ricerca https://air.uniud.it/. L'autrice riconduce a tale interpretazione la distinzione tra una trasparenza "*passiva e subìta*", a cui è soggetto il lavoratore osservato dal datore, da una trasparenza "*attiva e agìta*", di cui ci si propone la (ri)costruzione (opera ult. cit. p. 69).

Già nel 2019 l'OCSE ha pubblicato un documento, riguardante i principi sull'Intelligenza Artificiale, con l'obiettivo di promuovere una IA innovativa, capace di generare fiducia e rispettosa dei diritti umani. A tal fine, per OCSE i sistemi devono essere in grado di fornire informazioni significative per comprendere il sistema, rendere le parti coinvolte consapevoli delle loro interazioni con l'IA e di comprenderne il risultato, eventualmente anche per contestarlo[513].
Parimenti, il Libro bianco della Commissione europea sull'Intelligenza Artificiale[514], preludio della proposta legislativa europea in materia, identifica il principio di trasparenza tra i criteri fondamentali per ingenerare un ecosistema di fiducia verso IA.
L'articolo 13 della proposta di Regolamento su IA coerentemente sottolinea come i sistemi debbano essere progettati in modo che gli utenti interpretino e utilizzino le informazioni fornite dalla macchina e che queste vengano accompagnate da istruzioni che risultino complete e chiare. La norma precisa, inoltre, che i sistemi di Intelligenza Artificiale ad "alto rischio" debbano essere progettati e sviluppati in modo da garantire un livello di trasparenza sufficiente agli utenti per interpretare e utilizzare le informazioni acquisite.
In questo senso, gli strumenti di elaborazione dei dati, basati su sistemi di IA, dovranno garantire un livello di trasparenza adeguato affinché l'utente e il fornitore rispettino gli obblighi previsti dalla normativa.
Il medesimo orientamento è stato adottato dal Legislatore nazionale nel Decreto Trasparenza ove si impone al datore di lavoro l'obbligo di informare i lavoratori e i loro rappresentanti sul funzionamento degli algoritmi presenti nei sistemi automatizzati.

4.2. Ampliamento delle tutele collettive: diritto di informazione, negoziazione, consultazione e partecipazione attiva.

Il contesto tecnologico odierno in cui si sviluppano i rapporti di lavoro ha portato ad avvertire sempre più la necessità di un maggior coinvolgimento dei sindacati e dei rappresentanti dei lavoratori [515]quale misura di salvaguardia al (nuovo) potere datoriale.
È stato, infatti, osservato che "*la gestione algoritmica e l'esercizio del c.d. potere computazionale che discende dalle tecnologie abilitanti dell'Industria 4.0 creano un nuovo squilibrio contrattuale nel rapporto di lavoro (…) rispetto al quale si avverte una forte esigenza di tutela collettiva*"[516].

L'ampliamento auspicato delle tutele collettive parte da una collettivizzazione del diritto di informazione, così da favorire la procedimentalizzazione[517] dei poteri datoriali derivanti dalla datificazione del lavoro.
Allo stato attuale appare, infatti, privilegiata una visione ancora principalmente personalistica della tutela del diritto di informazione, soprattutto in riferimento all'utilizzo dei dati.

---

513 Punto 1.3 del documento OCSE "*Recommendation of the Council on Artificial Intelligence"* del 22.05.2019 consultabile sul sito https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449#_ga=2.84271514.264617860.1559118902-1252865362.1557825521

514 Libro Bianco della Commissione europea sull'Intelligenza Artificiale. Un approccio europeo all'eccellenza e alla fiducia, Bruxelles, 19.2.2020, COM(2020) 65 final.

515 Cfr. Piccinini I., Isceri M., *IA e datori di lavoro: verso una e-leadership?,* in *Lavoro Diritti Europa*, n. 2, 2021, p. 11; Iodice R., *La proposta di regolamento UE sull'Intelligenza Artificiale: quali implicazioni sul versante giuslavoristico?*, in *IANUS*, n. 24, 2021, pp. 55 ss.

516 Faleri C., *Brevi spunti di riflessione sull'evoluzione delle relazioni sindacali nell'economia digitale*, in *IANUS*, n. 24, 2021, p. 96; Zappalà L.; *Algoritmo*, in Borelli S, Brino V., Faleri C., Lazzeroni L, Tebano L., Zappalà L., *Lavoro e tecnologie. Dizionario del diritto del lavoro che cambia,* Giappichelli Editore, Torino, 2022, pp. 17 ss. In merito anche Dagnino E., *Dalla fisica all'algoritmo: una prospettiva di analisi giuslavoristica*, Adapt University Press, 2019.

517 Cfr. Zappalà L., *Appunti su linguaggio, complessità e comprensibilità del lavoro 4.0: verso una nuova procedimentalizzazione dei poteri datoriali*, in *WP CSDLE "Massimo D'Antona"*.it, n. 462, 2022.

L'informativa, la richiesta di spiegazioni e l'intervento di riesame umano, predisposti quali strumenti volti a controllare l'esercizio del potere datoriale, possono perdere la propria funzione di "limite esterno" ove non risultino azionati con sufficiente forza da parte del singolo.

Anche l'art. 4 SL[518], norma cardine sui controlli a distanza, pone un labile freno al potere di controllo subordinando l'utilizzabilità dei dati al rispetto dell'informativa sulle modalità di uso degli strumenti e di effettuazione dei controlli e sul rispetto della normativa *privacy*. Previsioni che possono risultare inadeguate[519] sia sul piano della trasparenza e dell'informativa preventiva (soprattutto in ragione del volume di dati acquisibili e della loro intellegibilità), sia per l'intervento oppositivo rimesso ai singoli prestatori.
La scelta di riporre la tutela nella normativa *privacy*, incentrata sull'iniziativa del singolo, "*denota una (forse inconscia) concezione liberale del rapporto di lavoro, collocando il prestatore su un piano di parità formale col datore di lavoro*"[520], trascurando la sua "*ontologica ed anzi progressiva debolezza contrattuale e sociale*" implementata da un divario sempre maggiore in virtù di una asimmetria informativa[521] e di comprensione degli strumenti digitali utilizzati.
I singoli lavoratori non dovrebbero, dunque, essere lasciati soli ad affrontare le complessità generate dalla tecnologia, soprattutto quando vogliono comprendere e contestare le decisioni algoritmiche e le conseguenze che queste possono apportare su di loro.

La previsione di obblighi di comunicazione indirizzati alla collettività dei lavoratori può, dunque, ricoprire un ruolo non solo preliminare di consultazione, ma anche di attiva partecipazione alla gestione organizzativa e di verifica dell'esercizio del potere datoriale.

Si rivela, pertanto, necessario definire in maniera differente il concetto di salvaguardia della trasparenza e del diritto di informazione nel contesto del lavoro digitale (e datificato), favorendo un intervento collettivo.
Ciò al fine di garantire che il potere datoriale generato dai dati segua un processo formale e dialogico, assicurando l'adozione di decisioni oggettive, giuste ed eque.
La collettivizzazione del diritto di informazione verrebbe, così, classificata come misura volta a ridurre non solo l'arbitrio del potere datoriale, ma anche l'opacità dello stesso ove trovi forza e fondamento nel controllo sui dati.
In tal senso si è mosso il Legislatore europeo nella proposta di Direttiva sulle condizioni di lavoro mediante piattaforme digitali che all'art. 9 prevede che le piattaforme digitali informino i lavoratori o i

[518] In merito è stato recentemente osservato che né l'art. 4 SL né la normativa *privacy* forniscono *"lo spazio che merita alla dimensione collettiva del problema del controllo a distanza (…) – non è mai un problema individuale del singolo lavoratore, ma una questione "indivisibile", che necessariamente coinvolge tutti i prestatori che si trovano nel medesimo luogo d'installazione delle apparecchiature"*. Ingrao A., *Controllo a distanza e privacy del lavoratore alla luce dei principi di finalità e proporzionalità della sorveglianza*, in *Labour & Law Issues (LLI),* vol. 9, n. 1, 2023, p. I. 116.
[519] Cfr. Tullini P., *Il controllo a distanza attraverso gli strumenti per rendere la prestazione a distanza*, in Tullini P. (a cura di) *Controlli a distanza e tutele dei dati personali del lavoratore*, G. Giappichelli Editore, Torino, 2017, p. 116.
[520] Garofalo D., *Prefazione,* in Zilli A., *La trasparenza nel lavoro subordinato. Principi e tecniche di tutela*, Pacini Giuridica, 2022, p. 11
[521]in merito, Faleri C., *Asimmetrie informative e tutela del prestatore di lavoro*, Giuffrè Editore, Milano, 2007 ove le asimmetrie informative vengono definite come una incrinatura nell'equità nei rapporti e nel mercato del lavoro; Zilli A., *La trasparenza nel lavoro subordinato. Principi e tecniche di tutela*, Pacini Giuridica, 2022. Sul piano di intervento normativo si richiama il nuovo art. 1-bis co. 4 del D. Lgs. 152/1997 che si ricollega espressamente l'art. 22 del GDPR. La norma richiamata esplicita come le decisioni datoriali passino anche attraverso elaborazioni algoritmiche o di sistemi di IA e che questi debbano palesarsi e rendersi comprensibili ai destinatari.

loro rappresentanti in merito alle "*decisioni che possono comportare l'introduzione o modifiche sostanziali nell'uso dei sistemi decisionali e di monitoraggio automatizzati*"[522].
Lo scopo di questa disposizione è, dunque, quello di promuovere il dialogo sociale sulla gestione algoritmica[523].

Parimenti, le novità introdotte dal D. Lgs n. 104 del 27 giugno 2022 (il cosiddetto Decreto trasparenza e sulle cui riflessioni si rinvia al capitolo precedente) relative ai nuovi obblighi informativi posti a carico del datore di lavoro in caso di utilizzo di sistemi automatizzati, ampliano la platea dei destinatari dell'informazione coinvolgendo anche le Parti sociali[524].

Ricevere adeguate informazioni diviene, quindi, il presupposto affinché le organizzazioni sindacali possano intervenire nel processo decisionale mediante gli strumenti di tutela collettiva da esse esperibili. Tale precisazione porta a distinguere quella che può essere una partecipazione cosiddetta "debole" del soggetto collettivo, che esaurisce la propria forza nel solo diritto di informazione, da una partecipazione "forte" che contempla un intervento attivo dei rappresentanti dei lavoratori nei processi decisionali[525].

Oltre ad una dimensione superindividuale dei diritti di informazione si dovrebbe, quindi, contestualmente procedere verso una proiezione collettiva delle tutele mediante uno sviluppo della negoziazione e della consultazione.
I diritti collettivi e la partecipazione dei lavoratori costituiscono, infatti, strumenti che possono divenire fondamentali per modellare in tal senso l'impiego della tecnologia nei rapporti di lavoro.
Partendo dalla negoziazione, tale prospettiva è stata già offerta dal GDPR ove, all'art. 88, afferma che gli Stati membri possono prevedere norme più specifiche per garantire la tutela dei diritti e delle libertà dei lavoratori per legge o per contratto collettivo[526].
Il potenziale della contrattazione collettiva può essere, dunque, valutato come mezzo per regolare l'impiego di algoritmi volti a elaborare dati dei lavoratori.
La peculiarità e molteplicità di modelli organizzativi che la digitalizzazione consente di introdurre, suggerisce di riconsiderare anche il sistema di negoziazione collettiva, portando a preferire un livello di contrattazione aziendale che meglio si adatti ai singoli contesti produttivi[527].
In particolare, il ruolo della contrattazione collettiva a livello aziendale può svilupparsi secondo una triplice direttiva[528]: innanzi tutto, per tutelare i diritti dei lavoratori secondo un modello di "contrattazione difensiva"; in secondo luogo, per favorire un "accompagnamento all'innovazione" prevedendo una contrattazione e a livello aziendale per consentire la formazione e lo sviluppo di competenze; infine, per

522 Art. 9 comma 1 proposta di Direttiva.
523 Cfr. De Stefano V., *Negotiating the Algorithm: Automation, Artificial Intelligence and Labour Protection*, in *Comparative Labor Law & Policy Journal,* vol. 41, n. 1, pp. 1 ss.
524 Art. 1bis comma 6 D. Lgs n. 152 del 1997, come modificato dal Decreto trasparenza, si legge che "*la comunicazione delle medesime informazioni e dati deve essere effettuata anche alle rappresentanze sindacali aziendali ovvero alla rappresentanza sindacale unitaria e, in assenza delle predette rappresentanze, alle sedi territoriali delle associazioni sindacali comparativamente più rappresentative sul piano nazionale*
525 In merito Biasi M., *Il nodo della partecipazione dei lavoratori in Italia*, Egea, 2013; Frosecchi G., *Diritti collettivi di informazione. Lezioni dal caso GKN,* in *Labour & Law Issues*, vol. 7, n. 2, 2021, pp. 43, 44.
526 Scelta che viene confermata anche dall'Accordo Quadro delle Parti Sociali Europee sulla digitalizzazione del giugno 2020 ove incoraggia le parti sociali a dare attuazione all'articolo 88 del GDPR prevedendo che negli accordi collettivi sia consentito "*ai rappresentanti dei lavoratori di affrontare le questioni relative ai dati, al consenso, alla tutela della privacy ed alla sorveglianza*" (p. 12). In merito Topo A., *Circolazione di informazioni, dati personali, profilazione e reputazione del lavoratore*, in Pisani C., Proia G., Topo A. (a cura di), *Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro*, Giuffrè Editore, Milano, 2022, pp. 389 ss.
527 Cfr. Faleri C., *Brevi spunti di riflessione sull'evoluzione delle relazioni sindacali nell'economia digitale*, in *LANUS*, n. 24, 2021, p. 108.
528 In merito si rinvia all'interessante riflessione offerta da Lucio Imberti nell'articolo *La contrattazione collettiva aziendale di fronte alle sfide della rivoluzione digitale e ai processi di cambiamento organizzativo*, in *Federalismi.it*, n. 25, 2022, pp.160 ss.

introdurre forme di "*partecipazione operativa ed organizzativa ai processi di innovazione dell'impresa*"[529] in una visione di "contrattazione proattiva".
A riguardo è stato osservato che, mentre la legislazione si rivela lo strumento migliore per fissare regole di base alle nuove pratiche gestionali, gli accordi collettivi sono il mezzo più idoneo a disciplinare il funzionamento degli apparati di sorveglianza[530].
I contratti collettivi hanno, infatti, il vantaggio di essere flessibili e di poter essere adattati nel tempo e al peculiare ambiente lavorativo a cui si applicano[531]. Risulterebbero, pertanto, degli strumenti di "*regolazione agile, capace di fronteggiare più efficacemente l'obsolescenza del diritto oggettivo*"[532].
Per questo motivo, oltre a un quadro legislativo generale predefinito, è essenziale una regolamentazione dettagliata e su misura. A questo proposito, la contrattazione collettiva può svolgere un ruolo primario, come appunto richiamato dall'art. 88 del GDPR.
Muovendo da tale presupposto, parte della dottrina auspica la stesura di un contratto collettivo sul trattamento dei dati dei lavoratori ove il datore di lavoro intenda esercitare un monitoraggio indiretto sui dipendenti[533].
Non sorprende, quindi, che si invochi un intervento efficace dei rappresentanti dei lavoratori per rafforzare le garanzie di trasparenza.
A questo proposito, il parere del Comitato economico e sociale europeo intitolato "*Creare fiducia nell'intelligenza artificiale antropocentric*a"[534] ha sottolineato la necessità di consultare e informare i lavoratori e i loro rappresentanti quando si introducono sistemi di Intelligenza Artificiale che potrebbero portare cambiamenti nell'organizzazione del lavoro, nella sorveglianza e nel controllo, così come nei sistemi di valutazione e assunzione dei lavoratori.
I contratti e gli accordi collettivi possono svolgere, pertanto, un compito fondamentale nel determinare le modalità, il contenuto e la periodicità di accesso alle informazioni relative ai parametri alle regole su cui si basano gli algoritmi utilizzati per prendere decisioni e che possono influenzare, direttamente o indirettamente, le condizioni di lavoro.
Questa prospettiva di intervento è quella prospettata dall'*European Social Partners Framework Agreement on Digitalisation*[535] il cui fine è quello di regolare in maniera condivisa l'introduzione degli strumenti digitali nell'organizzazione aziendale.
L'accordo propone di procedimentalizzare i poteri datoriali "tecnologici" così da favorire la cooperazione tra datore di lavoro e prestatori nella gestione degli strumenti informatici e limitandone gli effetti negativi.

---

529 Imberti L., *La contrattazione collettiva aziendale di fronte alle sfide della rivoluzione digitale e ai processi di cambiamento organizzativo*, in *Federalismi.it*, n. 25, 2022, p. 163.
530 Cfr. De Stefano V., '*Masters and Servers': Collective Labour Rights and Private Government in the Contemporary World of Work*, in *International Journal of Comparative Labour Law and Industrial Relations*, vol. 36, n. 4, 2020, pp. 425-444.
531 Cfr. De Stefano V., '*Negotiating the Algorithm': Automation, Artificial Intelligence and Labour Protection*, in *Comparative Labour Law & Policy Journal*, Vol. 41, n. 1, 2019, pp. 1-32; Faioli M., *Trasparenza e monitoraggio digitale. Perché abbiamo smesso di capire la norma sociale europea*, in *Federalismi.it*, del 5 ottobre 2022, n. 25, pp. 104 – 115; Tullini P., *Il controllo a distanza attraverso gli strumenti per rendere la prestazione lavorativa. Tecnologie di controllo e tecniche di lavoro: una distinzione possibile?,* in Tullini P. (a cura di), *Controlli a distanza e tutele dei dati dei lavoratori,* Giappichelli Editore, Torino, 2017, pp. 123 ss.
532 Topo A., Tardivo D., *Hard law e soft law nel diritto dell'Unione europea in materia di trattamento dei dati personali e di tutela della riservatezza del lavoratore*, in Pisani C., Proia G., Topo A. (a cura di), *Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro*, Giuffrè Editore, Milano, 2022, p. 105.
533 Cfr. Armaroli I, Dagnino E., *A Seat at the Table: Negotiating Data Processing in the Workplace*, in *Comparative Labour Law & Policy Journal*, vol. 41, n. 1, 2019, pp. 173-195.
534 Parere del Comitato economico e sociale europeo sulla comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni "*Creare fiducia nell'intelligenza artificiale antropocentrica*" [COM(2019) 168 final] punto 4.6.3.
535 Accordo sottoscritto il 22 giugno 2020 tra l'ETUC (*European Trade Union Confederation*) e le organizzazioni datoriali a livello europeo (Businesseurope, Ceep, Sme United).

Le fasi del processo descritte nell'Accordo prevedono in primo luogo un momento definito "*joint exploration/preparation/underpinning"* volto a creare una base condivisa per discutere le opportunità e i rischi connessi alla tecnologia che si intende introdurre.
La seconda fase, denominata "*joint mapping/regular assessment/analysis*", ha il fine di individuare congiuntamente le possibili misure e azioni volte a mitigare i rischi individuati.
La terza fase, definita "*joint overview of situation and adoption of strategies for digital transformation*", è quella in cui vengono concordate le strategie digitali e gli obiettivi dell'impresa.
La quarta fase, "*adoption of appropriate measures/actions*", prevede l'adozione delle misure individuate come adeguate a mitigare i pericoli.
Infine, l'ultima fase "*regular joint monitoring / follow-up, learning, evaluation*" è quella finalizzata a monitorare gli esiti del processo[536].
La "negoziazione dell'algoritmo"[537] la cui centralità è riconosciuta anche dalle Istituzioni[538] dovrebbe, quindi, diventare una questione centrale e il principale obiettivo del dialogo sociale.

Il rafforzamento di un'identità collettiva dei diritti di azione porta anche allo sviluppo di una fase consultiva, ossia di esame congiunto e dialogico tra sindacati e parte datoriale.
La previsione di un coinvolgimento dei rappresentanti dei lavoratori è presente nel dettato *de jure condendo* della proposta di Direttiva sul lavoro svolto mediante piattaforme digitali ove, all'art. 9, fa espresso riferimento al diritto di informazione e alla consultazione dei rappresentanti dei lavoratori (comma 1), richiamando la definizione di consultazione fornita dall'articolo 2, lettere f) e g), della Direttiva 2002/14/CE[539].
In merito è stato evidenziato[540] come nell'attuale versione della proposta di Direttiva, emendata dal Parlamento europeo nel 2023, vengano distinte le procedure di informazione e di consultazione rivolte ai singoli da quelle destinate alla collettività.
L'art. 9 della proposta di Direttiva compie plurimi rinvii alla Direttiva 2002/14/CE, inerente al diritto all'informazione e alla consultazione, incluse le definizioni da questa offerte.
Per "consultazione" si deve, dunque, intendere "*lo scambio di opinioni e l'instaurazione di un dialogo tra i rappresentanti dei lavoratori e il datore di lavoro*"[541].

---

536 *European Social Partners Framework Agreement on Digitalisation,* p. 7.
537 La terminologia "*Negotiating the algorithm*" viene utilizzata da Valerio De Stefano nel suo saggio *Negotiating the Algorithm: Automation, Artificial Intelligence and Labour Protection*, in *Comparative Labor Law & Policy Journal,* vol. 41, n. 1, p. 31. Parimenti Iolanda Piccinini e Marco Isceri parlano di "*contrattare l'algoritmo*". Piccinini I, Isceri M, *IA e datori di lavoro: verso una e-leadership?,* in *Lavoro diritti Europa*, n. 2, 2021, p. 15.
538 Nel 2019 l'OCSE ha adottato anche una raccomandazione in cui invita il dialogo sociale a svolgere un ruolo sull'introduzione e l'uso dell'intelligenza artificiale sul lavoro. Consiglio dell'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE) nella "*Raccomandazione sull'Intelligenza Artificiale (IA)*" del 22 maggio 2019 prononendo di "*rafforzare le capacità umane e prepararsi alla trasformazione del mercato del lavoro*" osserva che "*i governi dovrebbero adottare misure, anche attraverso il dialogo sociale, per garantire una transizione equa per i lavoratori man mano che l'intelligenza artificiale viene utilizzata, ad esempio attraverso programmi di formazione lungo la vita lavorativa, sostegno alle persone colpite dallo sfollamento e accesso a nuove opportunità nel mercato del lavoro*" (punto2.4 lettera b della Raccomandazione del Consiglio sull'intelligenza artificiale [OECD/LEGAL/0449]).
539 Direttiva 2002/14/CE del Parlamento Europeo e del Consiglio dell'11 marzo 2002 124 123 che istituisce un quadro generale per l'informazione e la consultazione dei lavoratori nella Comunità europea. La Direttiva prevede obblighi di informazione e consultazione sia su base *ad hoc*, sulle decisioni che possono comportare modifiche sostanziali nell'organizzazione del lavoro o nei rapporti contrattuali, sia, su base regolare, sull'evoluzione recente e probabile dell'impresa o della situazione attività e situazione economica dello stabilimento.
540 Purificato I., Senatori I., *The Position of Collective Rights in the 'Platform Work' Directive Proposal: Commission v Parliament*, in *Hungarian Labour Law E-Journal*, n. 1, 2023, pp. 14-18. Sul punto anche Otto M., *A step towards digital self- & co-determination in the context of algorithmic management systems*, in *Italian Labour Law e-Journal*, 2022, 2, p. 51 ss.; Delfino M., *Lavoro mediante piattaforme digitali, dialogo sociale europeo e partecipazione sindacale*, in *Federalismi.it,* n. 25, 2023, pp. 175,176.
541 Art. 2 lett. g) Direttiva 2002/14/CE. La medesima norma definisce come "informazione" la "*trasmissione di dati da parte del datore di lavoro ai rappresentanti dei lavoratori per consentir loro di prendere conoscenza della questione trattata e esaminarla*" (art. 2 lett. f)).

Nonostante la previsione della proposta di Direttiva sia da accogliere con favore, dato che prefigura una partecipazione attiva del soggetto collettivo alle decisioni datoriali, il rinvio compiuto dall'art. 9 alla Direttiva 2002/14/CE ha fatto riflettere la dottrina su una eventuale problematica applicazione pratica del diritto di consultazione, essendo essa rimessa alla contrattazione collettiva.
La contrattazione collettiva dei lavoratori su piattaforme rappresenta, infatti, "*un grande punto interrogativo, cosicché la normativa risulta di difficile applicazione al caso di specie*"[542].
La medesima dottrina auspica, dunque, che qualora la proposta di direttiva venga approvata senza ulteriori modifiche, affinché siano resi operativi i vincoli derivanti dalla Direttiva del 2002, vengano adattate "*le norme interne appena richiamate* (n.d.r. D. Lgs. 25/2007) *introducendo disposizioni che incentivino o sostengano la contrattazione collettiva nell'ambito del lavoro mediante piattaforme digitali oppure che prevedano un ruolo sostitutivo del legislatore*"[543].
La possibilità di riconoscere un rafforzamento dell'azione collettiva in termini di consultazione e, quindi, di coinvolgimento dell'organismo esponenziale potrebbe dunque trovare fondamento (con i dovuti adattamenti) nella previsione elaborata dalla proposta di Direttiva che delinea i diritti di informazione come propedeutici alla consultazione e al controllo sindacale dell'unità produttiva[544].
Come noto il D. Lgs. 25/2007, attuativo della Direttiva 2002/14/CE a cui rinvia l'art. 9 della proposta, prevede che "*le modalità di informazione e consultazione sono stabilite dal contratto collettivo*" (art. 1 comma 2) e che "*i contratti collettivi definiscono le sedi, i tempi, i soggetti, le modalità ed i contenuti dei diritti di informazione e consultazione*" (art. 4 comma 1).
Viene, dunque, rimessa alla contrattazione collettiva la definizione dei modi in cui la Parti Sociali devono essere informate e coinvolte dialogicamente nel processo decisionale.
La condivisione di informazioni, che consiste nella "*trasmissione di dati da parte del datore di lavoro ai rappresentanti dei lavoratori, finalizzata alla conoscenza ed all'esame di questioni attinenti alla attività di impresa*"[545] riguarda, infatti, anche "*le decisioni dell'impresa suscettibili di comportare rilevanti cambiamenti dell'organizzazione del lavoro e dei contratti di lavoro"*[546].
Il dettato normativo prevede, pertanto, una condivisione di informazioni e un successivo coinvolgimento delle rappresentanze dei lavoratori qualora le prerogative datoriali influiscano in maniera rilevante sull'organizzazione aziendale, come nel caso di un licenziamento collettivo.
In tale ipotesi, la procedura consultiva risulta necessaria e obbligatoria, ricevendo tutela autonoma in caso di violazione.

[542] Delfino M., *Lavoro mediante piattaforme digitali, dialogo sociale europeo e partecipazione sindacale*, in *Federalismi.it,* n. 25, 2023, p. 177.
[543] Delfino M., *Lavoro mediante piattaforme digitali, dialogo sociale europeo e partecipazione sindacale*, in *Federalismi.it,* n. 25, 2023, p. 177.
[544] Zilli A., *La trasparenza nel lavoro subordinato. Principi e tecniche di tutela*, Pacini Giuridica, 2022, pp. 133 ss.
[545] Art. 2, D. Lgs. n. 25/2007.
[546] Art. 4 comma 3 lettera c) D. Lgs. 25/2007.

Prospettiva riconosciuta dalla Giurisprudenza di merito del Tribunale di Firenze[547] che ha dichiarato antisindacale la condotta del datore di lavoro, il quale aveva omesso di coinvolgere le Parti Sociali nelle decisioni strategiche d'impresa, successivamente sfociate in un licenziamento collettivo[548].
Così riletti, gli obblighi di informazione "*assumono ben altra portata rispetto al mero adempimento della condivisione di informazioni (…) si giunge, infine, a valorizzarne il ruolo, quale tappa obbligata della consultazione e, financo, di una trattativa*"[549].

Alla luce di tali osservazioni, volgendo lo sguardo alla normativa nazionale di recente introduzione in materia di condizioni di lavoro trasparenti e prevedibili dei sistemi decisionali e di monitoraggio automatizzati (in merito ai quali si rinvia a quanto detto nel quarto capitolo), si nota l'assenza di un esplicito riferimento alla consultazione.
Il D. Lgs. 104/2022, infatti, pur introducendo una dimensione collettiva della garanzia di informazioni per i sistemi automatizzati implementati in azienda non è, però, "*riuscito a cogliere l'occasione per inserire accanto al diritto informativo della RSU un obbligo di consultazione sindacale in questa materia*"[550].
La norma citata, infatti, pur riconoscendo una titolarità collettiva dei diritti di informazione, si astiene dal definire un diritto di consultazione delle rappresentanze dei lavoratori.
Il ruolo attivo dei sindacati rimane, quindi, limitato a una sfera meramente informativa, sicuramente di rilievo e propedeutica all'esercizio delle tutele collettive, ma insufficiente a legittimare il soggetto collettivo ad agire *iure proprio* in caso di mancato coinvolgimento nei processi decisionali datoriali.
L'art. 1 *bis* del Decreto trasparenza riconosce, in sostanza, il diritto ai sindacati a essere informati in modo adeguato sull'implementazione dei sistemi automatizzati, ma non si pronuncia in merito a una successiva fase di consultazione in cui i rappresentanti dei lavoratori possano esprimere pareri e proposte sull'utilizzo di tali sistemi.
Conseguentemente, mentre la violazione dei doveri informativi determina una condotta antisindacale, azionabile direttamente dell'organismo esponenziale ai sensi dell'art. 28 dello Stato dei Lavoratori, tale via non sarebbe esperibile in caso di mancata consultazione delle rappresentanze.

---

547 Il riferimento è al caso *GKN Driveline* di Campi Bisenzio, oggetto del Decreto emesso dal Tribunale di. Firenze il 20 settembre 2021 ai sensi dell'art. 28 Stat. Lavoratori. Nello specifico, il Tribunale ha riconosciuto la condotta antisindacale dell'impresa GKN per mancato avvio delle procedure di consultazione e confronto previste dal CCNL delle aziende metalmeccaniche. Il comportamento antisindacale accertato è consistito, dunque, "*nella sua parte più significativa e lesiva degli interessi del sindacato ricorrente, nell'aver impedito al sindacato stesso di interloquire, come sarebbe stato suo diritto, nella delicata fase di formazione della decisione di procedere alla cessazione totale dell'attività di impresa*" (Ordinanza Tribunale di Firenze del 20.09.2021 p. 7). In merito Zilli A, *La trasparenza nel lavoro subordinato. Principi e tecniche di tutela*, Pacini Giuridica, 2022, p. 118.; Corti M. *Il coinvolgimento dei lavoratori preso sul serio: il caso GKN,* in *Diritto delle Relazioni Industriali (DRI),* n. 1, 2022, pp. 265 ss.; Peruzzi M., *Intelligenza Artificiale e lavoro. Uno studio su poteri datoriali e tecniche di tutela*, Giappichelli Editore; Torino, 2023, pp. 92, 93; Frosecchi G., *Diritti collettivi di informazione. Lezioni dal caso GKN,* in *Labour & Law Issues (LLI*), vol. 7, n. 2, 2021, pp. 37 ss.
548 La fase di consultazione sarebbe, dunque, precedente e ulteriore rispetto a quella prevista dalla Legge n. 223/1991 in materia di licenziamenti collettivi, avendo ad oggetto il coinvolgimento dei rappresentanti dei lavoratori nelle decisioni strategiche aziendali.
549 Zilli A, *La trasparenza nel lavoro subordinato. Principi e tecniche di tutela*, Pacini Giuridica, 2022, p. 118.
550 Ingrao A., *Controllo a distanza e privacy del lavoratore alla luce dei principi di finalità e proporzionalità della sorveglianza*, in *Labour & Law Issues (LLI),* vol. 9, n. 1, 2023, p. I 118. Parimenti Giuseppe Antonio Recchia osserva che "*resta fuori, almeno per il momento, il passaggio successivo all'informazione, ovvero la consultazione sindacale, come prevede l'art. 9 della Proposta di Direttiva che la garantisce (limitatamente però ai lavoratori delle piattaforme qualificabili come subordinati) quale momento di partecipazione preventiva rispetto alle «decisioni che possono comportare l'introduzione o modifiche sostanziali nell'uso dei sistemi decisionali e di monitoraggio automatizzati*" Recchia G. A., *Condizioni di lavoro trasparenti, prevedibili e giustiziabili*, in *Labour & Law Issues (LLI),* vol. 9, n. 1, 2023, p. C. 45, nota 40.

Ricostruzione fatta propria anche dalla recente Giurisprudenza di merito del tribunale di Palermo[551] e di Torino[552] che qualifica come condotta antisindacale l'omessa informativa richiesta, ai sensi dell'art. 1 *bis* comma 6 del Decreto trasparenza, dalle rappresentanze in merito ai sistemi automatizzati impiegati.
Nulla in più si può, però, dire in riferimento a un omesso coinvolgimento consultivo delle Parti sociali mancando un espresso obbligo in tal senso.
Vi sono, dunque, ancora spazi di sviluppo per agevolare lo scambio di opinioni e l'instaurazione di un dialogo tra le parti.

L'evoluzione delle tutele collettive passa, infine, anche attraverso nuove forme partecipative[553] e non solo su modelli di consultazione e contrattazione.
Se è vero, infatti, che l'intervento delle Parti sociali si mostra quale forma più duttile per rispondere alle nuove esigenze di adattamento a una realtà in continuo cambiamento, le forme partecipative avrebbero il ruolo di integrare e rafforzare tali tutele.
La digitalizzazione e datificazione del lavoro impongono, infatti, "*un ripensamento non solo delle strutture della partecipazione, ma dei suoi ambiti di intervento e delle sue condizioni di successo. Questo perché gli interventi delle macchine pongono una sfida inedita alle parti delle relazioni industriali, nella loro attività contrattuale, come nelle forme partecipative*"[554].
Le forme partecipative di intervento delle Parti sociali potrebbero, inoltre, ricoprire un ruolo preliminare[555], attuandosi prima dell'impiego della tecnologia se non, addirittura, inserendosi nel momento della sua programmazione. Ciò consentirebbe di definire in maniera congiunta la finalità di impiego.

---

551 In merito Tribunale di Palermo, Ordinanza del 3 aprile 2023, n. 14491. Sul punto il Tribunale afferma che "*l'art. 1 bis, introdotto dall'art. 4 d. lgs. 104/2022, prevede che "Il datore di lavoro o il committente pubblico e privato è tenuto a informare il lavoratore dell'utilizzo di sistemi decisionali o di monitoraggio automatizzati deputati a fornire indicazioni rilevanti ai fini della assunzione o del conferimento dell'incarico, della gestione o della cessazione del rapporto di lavoro, dell'assegnazione di compiti o mansioni nonché indicazioni incidenti sulla sorveglianza, la valutazione, le prestazioni e l'adempimento delle obbligazioni contrattuali dei* lavoratori" ed allora, considerato che la legittimazione attiva alla richiesta di informazioni compete non soltanto al *lavoratore ma anche alle RSA, RSU o alle associazioni sindacali comparativamente più rappresentative, il relativo diniego limita e compromette l'attività sindacale, legittimando la richiesta di rilascio delle informazioni ex art. 28, integrando già lo stesso rifiuto datoriale una lesione del diritto alla informativa azionabile anche da parte sindacale, quindi in aggiunta e non in alternativa rispetto all'eventuale previo rilascio al lavoratore, ragion per cui nessuna rilevanza assume la difesa della convenuta di aver già fornito le informazioni richieste ai lavoratori*". Sul punto Peruzzi M., *Intelligenza Artificiale e lavoro. Uno studio su poteri datoriali e tecniche di tutela,* Giappichelli Editore, Torino, 2023, p. 93.; Recchia G. A., *Condizioni di lavoro trasparenti, prevedibili e giustiziabili*, in *Labour & Law Issues (LLI),* vol. 9, n. 1, 2023, pp.C.33 ss.
552 Tribunale di Torino, Decreto del 5 agosto 2023 il quale ha ritenuto le informazioni fornite dalla società convenuta "*non (…) sufficienti per poter ritenere adempiuto l'obbligo informativo di cui all'art. 1 bis del d.lgs. 152/1997*" (p. 29 del Decreto) e conseguentemente ha dichiarato antisindacale il comportamento tenuto dalla società datrice di lavoro consistito nel rifiuto di comunicare alle OO.SS. ricorrenti le informazioni richieste di cui all'articolo 1 bis del d.lgs. 152/1997.
553 Nonostante l'art. 46 della Costituzione, che riconosce il diritto dei lavoratori a collaborare alla gestione delle aziende "*nei modi e nei limiti stabiliti dalle leggi*", è rimasto sostanzialmente inattuato esistono alcuni modelli "latentemente partecipativi" (come definiti da Anna Zilli in *La trasparenza nel lavoro subordinato. Principi e tecniche di tutela*, Pacini Giuridica, 2022, p. 114) basati sulla condivisione di informazioni. tra questi quello proposto dal D. Lgs. n. 25/2007 di attuazione della Direttiva 2002/14/CE e il D.Lgs. n. 81/2008 in materia di salute e sicurezza sul lavoro. In merito Zoppoli L., *Modelli partecipativi e tecniche di regolazione dei rapporti di lavoro*, in *Diritto delle Relazioni Industriali (DRI),* vol. 20, n. 1, 2010, pp. 19 ss; Alaimo A., *l'eterno ritorno della partecipazione: il coinvolgimento dei lavoratori al tempo delle nuove regole sindacali*, in *Biblioteca 20 Maggio,* 2/2014 (Originariamente pubblicato come *WP C.S.D.L.E. "Massimo D'Antona".it* – 219/2014), pp. 1 ss.
554 Treu T., *La digitalizzazione del lavoro: proposte europee e piste di ricerca*, in Federalismi.*it*, focus, lavoro, tecnologia, persona, marzo 2022, p. 203.
555 Per parte della dottrina risulta quindi "*indispensabile che il sindacato intervenga, fin dalla fase di progettazione dell'algoritmo, sui meccanismi di funzionamento automatico dei sistemi predittivi in modo da ricondurli – tramite la valorizzazione e l'implementazione dei principi di trasparenza e di conoscibilità dei meccanismi decisionali automatizzati – alla capacità di controllo e di orientamento umano affinché equità e qualità dei rapporti di lavoro nell'economia digitale possano essere credibilmente perseguite*" Faleri C., *Brevi spunti di riflessione sull'evoluzione delle relazioni sindacali nell'economia digitale*, in *IANUS*, n. 24, 2021, p. 106. In merito anche Treu T., *La digitalizzazione del lavoro: proposte europee e piste di ricerca*, in *federalismi.it*, n. 9, 2022, 190 ss.

Soluzione che, per certi versi, ritrova già nel dettato dell'art. 4 SL[556] una matrice che nella sua originaria versione del 1970, successivamente depotenziata[557] dalla riforma, proponeva un modello di partecipazione dei lavoratori alla gestione delle imprese.

Il coinvolgimento dei lavoratori e dei loro rappresentanti avverrebbe, in tal modo, non solo *ex post*, con finalità di mero controllo di funzionamento della tecnologia, ma verrebbe anticipato intervenendo fin dal momento di pianificazione strategica dell'uso di strumenti digitali in azienda.
L'azione sindacale "*da reattiva dovrebbe così diventare più preventiva, predittiva e progettuale*"[558].

Esempi virtuosi di modelli partecipativi nell'ambito delle relazioni industriali sono stati oggetto di analisi dottrinale[559] e propongono un prototipo di dialogo che si impernia su "*un sistema di confronto continuo, finalizzato alla ricerca di soluzioni anche possibilmente concordate, con il quale prevenire e comunque affrontare tutte le problematiche che emergono dallo sviluppo del processo con l'obiettivo comune del miglioramento"*[560].

La realizzazione di una strategia di IA affidabile non può, quindi, fermarsi all'adozione di una regolamentazione europea, ma richiede la tessitura di una trama sociale che, in modo flessibile, intrecci le tutele giuslavoristiche con quelle di protezione dei dati, mediante l'impiego di strumenti di consultazione, negoziazione e partecipazione collettiva.
Indicazioni che possono trovare una sede adeguata non solo all'interno di testi normativi, ma anche nel dialogo sociale.

L'Accordo quadro europeo sul tema sul tema della digitalizzazione del 2020 sembra aver colto tale necessità e suggerisce di "*sperimentare codici di condotta e linee guida pariteticamente costituite dalle organizzazioni sindacali, dal management e dalle Autorità di vigilanza competenti per garantire, fin dalla prima fase di progettazione della macchina intelligente, il diritto di informazione e consultazione sindacale ai lavoratori che si interfacceranno con gli strumenti di AI*"[561].
Sulle linee di intervento proposte dall'Accordo europeo, parte della dottrina propone soluzioni partecipative innovative, come la creazione di "*comitati paritetici misti datore/rappresentanti dei lavoratori*"[562] con il compito di valutare l'operato e gli eventuali errori commessi dai sistemi di IA impiegati, idonei ad arrecare danno a sicurezza, libertà e dignità umana.

---

556 In merito le riflessioni di Alessandra Ingrao la quale, in riferimento alle minacce derivanti dalla tecnologia e alle tutele offerte dall'art. 4 SL, osserva che la norma citata già conteneva l'intuizione su come fronteggiare tali criticità mediante due vie. "*La prima è quella della partecipazione dei lavoratori alla gestione delle imprese, sub specie di partecipazione alla gestione, miglioramento e umanizzazione delle prerogative tecnologiche dell'impresa. La seconda è quella che fa leva sul principio di prevenzione e trasparenza*". Ingrao A., *Riflessioni intorno alla partecipazione dei lavoratori nell'era dell'algoritmo, alla luce dell'accordo Just Eat- Takeaway.com*, in Mingione E., Scarpelli F., Giasanti L. (a cura di), *Lo Statuto dei lavoratori alla prova dell'oggi: Una rilettura critica da parte degli studiosi di nuova generazione,* Feltrinelli, Milano, 2022, *p. 115*. Consultabile al *link: https://fondazionefeltrinelli.it/app/uploads/2022/11/Finale_StatutoLavoratori-1.pdf.*

557 Cfr. Ingrao A., *Riflessioni intorno alla partecipazione dei lavoratori nell'era dell'algoritmo, alla luce dell'accordo Just Eat- Takeaway.com*, in Mingione E., Scarpelli F., Giasanti L. (a cura di), *Lo Statuto dei lavoratori alla prova dell'oggi: Una rilettura critica da parte degli studiosi di nuova generazione, Feltrinelli, Milano, 2022, pp. 121 ss.* Consultabile al *link: https://fondazionefeltrinelli.it/app/uploads/2022/11/Finale_StatutoLavoratori-1.pdf.*

558 Faleri C., *Brevi spunti di riflessione sull'evoluzione delle relazioni sindacali nell'economia digitale*, in *IANUS*, n. 24, 2021, p. 106.

559 I casi sono quelli di Sidel S.p.A. e di CB Ferrari S.r.l. analizzati da Licio Imberti nel saggio., *La contrattazione collettiva aziendale di fronte alle sfide della rivoluzione digitale e ai processi di cambiamento organizzativo*, in *Federalismi.it*, n. 25, 2022, pp. 160 ss.

560 Imberti L., *La contrattazione collettiva aziendale di fronte alle sfide della rivoluzione digitale e ai processi di cambiamento organizzativo*, in *Federalismi.it*, n. 25, 2022, p. 165.

561 Cappellazzo N., *L'art. 8 Stat. Lav. e i meccanismi di HR algorithms management: lo Statuto dei lavoratori alla prova delle nuove tecnologie*, in *Federalismi.it* del 9 agosto 2023, n. 21/2023, p. 203.

562 Piccinini I., Isceri M., *IA e datori di lavoro: verso una e-leadership?,* in *Lavoro Diritti Europa*, n. 2, 2021, p. 19.

Altra parte della dottrina[563], volgendo lo sguardo verso altri paesi europei, riporta testimonianze di modelli di coinvolgimento dei rappresentanti dei lavoratori che attuano modelli codecisionali quando siano coinvolti sistemi di Intelligenza Artificiale.

L'intervento preventivato delle Parti sociali consentirebbe, dunque, di regolamentazione l'utilizzo della tecnologia secondo un approccio condiviso di cooperazione tra datore di lavoro, prestatori e fornitori del servizio di IA così da comprendere, prima dell'inserimento e utilizzo dei sistemi di elaborazione, le situazioni potenzialmente lesive dei diritti dei lavoratori[564].

Il riconoscimento di un'azione collettiva volta a tutelare gli interessi dei lavoratori trova riscontro anche nel dettato del GDPR ove conferisce a organismi esponenziali la possibilità di dare voce ai diritti degli interessati, prevedendo anche la facoltà che sia loro attribuita una legittimazione diretta.
Il Regolamento in tema dei mezzi di tutela collettivi per la protezione dei dati mostra, infatti, un certo *favor*[565] a partire dall'art. 80 del GDPR.
La norma citata al primo comma consente, infatti, agli interessati di presentare reclami e agire per conto degli stessi dando mandato a organizzazioni o associazioni "*senza scopo di lucro, che siano debitamente costituiti secondo il diritto di uno Stato membro, i cui obiettivi statutari siano di pubblico interesse e che siano attivi nel settore della protezione dei diritti e delle libertà degli interessati con riguardo alla protezione dei dati personali*".
Il medesimo articolo al secondo comma attribuisce alle medesime organizzazioni o associazioni di intentare azioni collettive per conto degli interessati al fine di far valere i loro diritti in materia di protezione dei dati.
La norma pone, dunque, particolari organismi esponenziali quali interlocutori diretti del titolare del trattamento, abilitati a promuovere e tutelare i diritti degli interessati, nonché a compiere azioni superindividuali.
La previsione ammette, in tal modo, una tutela collettiva ove i diritti dei singoli interessati non trovino adeguata salvaguardia mediante l'azione individuale, riconoscendo la posizione di maggior soggezione dell'interessato nei riguardi del titolare del trattamento.
Prospettiva che *a fortiori*, dovrebbe valere nell'ambito di un rapporto di lavoro tradizionalmente definito come "squilibrato" e in cui lo *status* del prestatore risulta "debole"[566] nei confronti del datore di lavoro.
Il Regolamento posto a tutela dei dati personali prevede, inoltre, che qualora si introduca un processo automatizzato, il titolare del trattamento sia tenuto a compiere una valutazione di impatto, ai sensi dell'art. 35, par. 9 GDPR.

---

563 In merito si riporta l'interessante studio comparativo proposto da Matteo Corti sui sistemi di tutela collettivi vigenti in Italia e Germania. L'autore osserva come "*i diritti di codecisione garantiti al consiglio d'azienda nelle materie sociali e del personale trovano applicazione anche quando siano coinvolti sistemi di intelligenza artificiale, consentendo ai rappresentanti dei lavoratori di governarne l'introduzione e applicazione*". Corti M., *Potere di controllo e nuove tecnologie. Il ruolo dei partner sociali,* in *Labour & Law Issues (LLI),* vol. 9, n.1, 2023, p. I 68.

564 Approccio *button-up*. In questo senso cfr Rudin V. C., *Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead,* in *Nat Mach Intell*, n. 1, 2019, p. 206–215; Cappellazzo N., *L'art. 8 Stat. Lav. e i meccanismi di HR algorithms management: lo Statuto dei lavoratori alla prova delle nuove tecnologie*, in *Federalismi.it* del 9 agosto 2023, n. 21/2023, p. 2014.

565 In merito si rinvia all'interessante riflessione offerta da Simone Scagliarini nell'articolo, *La tutela della privacy e dell'identità personale nel quadro dell'evoluzione tecnologica,* in *Consulta OnLine*, n. 2, 2021, pp. 597-599.

566 Visione espressa anche dalla Corte costituzionale n. 99 del 19 giugno 1980 per cui il rapporto di lavoro è connotato da un "*inevitabile e irriducibile contrasto fra datori di lavoro e lavoratori*", nonché da "*un incessante conflitto fra opposti interessi degli uni e degli altri*". Parole riprese anche dal Tribunale di Firenze nella sentenza del 20 settembre 2021 sul caso GKN.

Disposizione che trova ulteriore riscontro nella proposta di Direttiva sul lavoro sulle piattaforme digitali[567] che rafforza tale adempimento, come si ha avuto modo di approfondire nel terzo capitolo a cui si rinvia.
Il datore di lavoro nell'espletare l'adempimento della DPIA si trova, così, nella condizione di verificare la necessità di un eventuale confronto con i rappresentanti dei soggetti interessati, ovvero i lavoratori[568].
Allo stesso modo, anche il Considerando 99 del GDPR, in tema di Codici di condotta, apre la strada ad una partecipazione di organismi rappresentanti le categorie degli interessati.
Indicazione che può essere intesa "*come necessaria misura procedimentale, coinvolgendo anche dal lato delle categorie di interessati le associazioni di rappresentanza*"[569].

La dimensione collettiva delle tutele porta, quasi inevitabilmente, a presumere un nesso tra diritti sociali e diritti del lavoro volto a stimolare l'intervento anche delle istituzioni.
Il soggetto pubblico può, infatti, giocare un ruolo suppletivo, ricomponendo e tutelando gli interessi dei lavoratori, qualora non sia presente sul posto di lavoro una rappresentanza sindacale.
In particolare, richiamando lo schema di tutele proposto dall'art. 4 dello Statuto dei Lavoratori, anche in questo caso l'organo amministrativo potrebbe ricoprire un ruolo sostitutivo, aprendo uno spazio di negoziazione assistita ove l'azione individuale non risulti efficace e manchi la rappresentanza di un soggetto collettivo.
L'art. 4 SL prevede, infatti, che in mancanza di un accordo - dovuto ad assenza delle rappresentanze o per fallita contrattazione con le associazioni sindacali - il datore di lavoro possa promuovere istanza all'Ispettorato Nazionale del Lavoro[570] al fine di ottenere l'autorizzazione per installare[571] gli strumenti di controllo.
Il ruolo riconosciuto dalla norma all'Ispettorato è quello di accertare la sussistenza dei presupposti indicati dall'art. 4 SL (ossia la fondatezza delle esigenze organizzative, produttive, di sicurezza del lavoro o di tutela del patrimonio aziendale), nonché il rispetto della normativa *privacy*.
Parimenti, anche in questo caso l'intervento amministrativo andrebbe in supporto di quelle tutele che, ove riconosciute di interesse collettivo, rimangano inermi in assenza di un organo esponenziale che le azioni, riequilibrando il rapporto tra le parti.

---

567 La piattaforma è, per esempio, tenuta a raccogliere il parere dei rappresentanti dei lavoratori sul trattamento previsto (articolo 6, paragrafo 5 bis), coinvolgerli nella valutazione (articolo 7, paragrafo 1) e presentare il documento finale compilato (articolo 7, paragrafo 2bis). L'invito a ricorrere alla consultazione collettiva viene, inoltre, evidenziato dal nuovo paragrafo 2bis dell'art. 9 ove si legge che "*le piattaforme di lavoro digitali forniscono ai rappresentanti dei lavoratori le informazioni di cui all'articolo 6, paragrafi 1, 2, 5 bis e 5 ter, e all'articolo 7 in tempo utile per consentire un esame approfondito e una consultazione efficace (…)*".
568 In merito Peruzzi M., Intelligenza artificiale e lavoro. Uno studio su poteri datoriali e tecniche di tutela, Giappichelli Editore, Torino, 2023, pp. 83 ss.
569 Scagliarini S., *La tutela della privacy e dell'identità personale nel quadro dell'evoluzione tecnologica,* in *Consulta OnLine*, n. 2, 2021, p. 598.
570 A seconda dei casi nella sede territoriale o centrale. Art. 4 comma 1 SL. In forza del Decreto legislativo n. 149/2015, dal 14 settembre 2015, è stata istituita l'Agenzia unica per le ispezioni del lavoro denominata "Ispettorato Nazionale del Lavoro" che "esercita e coordina sul territorio nazionale la funzione di vigilanza in materia di lavoro, contribuzione, assicurazione obbligatoria e di legislazione sociale, compresa la vigilanza in materia di tutela della salute e della sicurezza nei luoghi di lavoro" (così definita dal Ministero del Lavoro e delle Politiche Sociali sul sito visionabile al seguente link. https://www.lavoro.gov.it/temi-e-priorita/salute-e-sicurezza/focus-on/attivita-ispettiva/pagine/default#:~:text=In%20base%20alle%20direttive%20emanate,sicurezza%20nei%20luoghi%20di%20lavoro).
571 L'interesse all'installazione può sussistere per alcuni autori anche in capo alle stesse rappresentanze dei lavoratori (RSA/RSU). In tal senso si rinvia a Maio V., *Il regime delle autorizzazioni del potere di controllo del datore di lavoro ed i rapporti con l'art. 8 della legge n. 148/2011,* in Tullini P. (a cura di), *Controlli a distanza e tutele dei dati personali del lavoratore*, G. Giappichelli Editore, Torino, 2017, p. 91, riportato anche in nota da Ingrao A., *Il controllo a distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata*, Cacucci Editore, Bari, 2018, p. 200.

In tal senso può essere letta la previsione introdotta dal nuovo art. 1 bis[572] del D. Lgs. 152 del 1997, ove si prevede che l'Ispettorato del Lavoro può richiedere informazioni oggetto del dovere di trasparenza al datore di lavoro nel caso di utilizzo di sistemi decisionali o di monitoraggio automatizzati, anche se con funzione più di accertamento per eventuali infrazioni che di coinvolgimento rispetto a quella destinata ai soggetti rappresentativi dei lavoratori[573].
Disposizione che, in ogni caso, riconosce al soggetto pubblico un ruolo di garanzia a tutela degli interessi dei lavoratori.
La *ratio* di un eventuale intervento dell'Ispettorato si potrebbe, dunque, rinvenire nel limite posto alla facoltà di disposizione dei diritti da parte del lavoratore, al pari di quanto previsto in tema di rinunce e transazioni dall'art. 2113 del Cod. Civile[574].

4.3. Sviluppo di strumenti di "*soft law*": i Codici di condotta

In accordo con il punto precedente, le tutele dei lavoratori possono prevedere l'adozione di specifici Codici di condotta che agevolino i diritti di informazione.
La proposta di Regolamento su IA, al fine di implementare la gestione umana dei sistemi di Intelligenza Artificiale in una prospettiva "antropocentrica", introduce all'art. 69[575] la disciplina dei Codici di condotta.
La previsione di Codici di condotta quali "*strumenti di responsabilizzazione volontari che stabiliscono specifiche norme di protezione*"[576] si ritrova anche in materia di protezione dei dati personali.
L'art. 40 del GDPR prevede, infatti, l'obbligo per alcuni enti ed istituzioni di incoraggiare le associazioni o gli organismi rappresentanti categorie di titolari di trattamento a elaborare questi documenti per contribuire alla corretta applicazione del Regolamento, tenendo conto dei vari settori e delle esigenze di ogni impresa[577].
La redazione e il rispetto di un Codice di condotta, approvato ai sensi dell'art. 40 GDPR può, dunque, essere un elemento volto a dimostrare che sono state scelte e introdotte misure adeguate.
Analogamente, la proposta di Regolamento su IA prevede che gli Stati membri promuovano la volontaria redazione di Codici di condotta con lo scopo di applicare ai sistemi di IA non ad alto rischio le azioni

---

572 All'art. 1 bis, comma 6 D. Lgs. 152 del 1997 (introdotto dal c.d. Decreto trasparenza) si legge infatti che *"(…) Il Ministero del lavoro e delle politiche sociali e l'Ispettorato nazionale del lavoro possono richiedere la comunicazione delle medesime informazioni e dati e l'accesso agli stessi"*.

573 In merito è stato osservato che "*con riferimento ai rappresentanti dei lavoratori, l'informativa serve a permettere un controllo più penetrante e consapevole di quello che potrebbe essere effettuato dal singolo lavoratore per accertare se l'algoritmo è rispettoso della legge (il soggetto collettivo infatti ha le capacità economiche anche per dotarsi di consulenti), inoltre le informazioni possono dar avvio ad una fase di contrattazione per riformulare/correggere il "sistema automatizzato" così da limitare ulteriormente il potere datoriale informatizzato oltre quanto prescritto dalle norme; con riferimento ai soggetti pubblici, invece, l'informativa serve per un più agevole accertamento di eventuali infrazioni, poi soggette alle sanzioni amministrative di cui all'art. 4 d.lgs. n. 152/1997"*. Carinci M. T., Giudici S., Perri P., *Obblighi di informazione e sistemi decisionali e di monitoraggio automatizzati (art. 1-bis "Decreto Trasparenza"): quali forme di controllo per i poteri datoriali algoritmici?,* in *Labor*, n. 1, 2023, p. 23.

574 L'art. 2113 del Cod. Civ. prevede infatti che "*Le rinunzie e le transazioni, che hanno per oggetto diritti del prestatore di lavoro derivanti da disposizioni inderogabili della legge e dei contratti o accordi collettivi concernenti i rapporti di cui all'articolo 409 del Codice di procedura civile, non sono valide*" (comma 1). La norma prosegue all'ultimo comma precisando che "*Le disposizioni del presente articolo non si applicano alla conciliazione intervenuta ai sensi degli articoli 185, 410, 411, 412-ter e 412-quater del Codice di procedura civile.*
L'invalidità nascerebbe dalla volontà del legislatore di sottrarre al lavoratore, titolare dei diritti, la possibilità di disporne. Scelta volta non solo a tutelare il singolo, ma anche l'interesse collettivo dei lavoratori. In tal senso cfr. De Luca Tamajo R., *La norma inderogabile nel diritto del lavoro*, Editore Jovene, Napoli, 1976; Fabris P., *L'indisponibilità dei diritti dei lavoratori*, Giuffrè Editore, Milano, 1978.

575 Titolo IX della Proposta di Regolamento fatta dalla Commissione nel 2021 in materia di Intelligenza Artificiale.

576 European Data Protection Board (EDPB) Linee guida 1/2019 sui codici di condotta e sugli organismi di monitoraggio a norma del regolamento (UE) 2016/679 del 4.6.2019.

577 Ai sensi dell'art. 24 par. 3 del GDPR l'adesione ad un Codice di condotta può costituire un mezzo per dimostrare, nell'ottica del principio accountability, l'applicazione del Regolamento europeo da parte del Titolare del trattamento dei dati personali.

positive indicate nel titolo III, capo 2, ossia quelle obbligatorie che i fornitori di IA ad alto rischio devono applicare per mitigarne gli effetti nocivi delle macchine.
La disciplina sui Codici di condotta non riporta modifiche sostanziali anche a seguito dell'emendamento introdotto dal Consiglio dell'Unione europea nel settembre del 2022, mantenendo la natura di "*soft law*" dei codici.
Amplia, però, la platea di soggetti che possono elaborarli, includendo i sindacati[578].

L'introduzione e la diffusione dei Codici di condotta potrebbe essere la chiave per favorire l'adozione di prassi virtuose orientate ad un *Human Rights Approach*[579] e che agevolino il coinvolgimento dei soggetti interessati, facilitando la trasparenza dei sistemi e la sorveglianza umana.
Proprio la flessibilità della redazione dei Codici potrebbe consentire di implementare, a seconda delle peculiarità di ogni IA, le fasi di intervento umano, aiutando la comprensione dei sistemi e implementando le informazioni impiegate per rendere motivazioni esaustive.
I Codici di condotta potrebbero, inoltre, favorire la corretta selezione e interpretazione degli *output* elaborati, evitando la realizzazione di *bias* e consentendo di interrompere le operazioni di analisi ove contravvengano i limiti indicati.
In particolare, per garantire una corretta interpretazione degli *output*, quali possono essere le analisi dei dati "non autoevidenti", potrebbero essere stabiliti il modo in cui il risultato viene condiviso con i lavoratori, le fasi di comunicazione e i soggetti destinatari (ossia il singolo prestatore, i rappresentanti o delegati dotati di particolari competenze).
In Codici di condotta potrebbero, quindi, favorire la forma partecipativa dei lavoratori non solo nell'utilizzo dei sistemi automatici, ma anche nel preliminare studio finalizzato a pianificarne l'introduzione in azienda, nonché il loro aggiornamento.
Parimenti, potrebbero garantire l'accesso ai mezzi di impugnazione delle decisioni algoritmiche, garantendo il corretto *iter* di contestazione e la tempistica di intervento.
L'impiego di Codici di condotta potrebbe incidere, dunque, non solo sul rispetto dei diritti dei lavoratori, ma anche sulla progettazione e programmazione dei sistemi di IA in forza di una maggiore conoscenza degli interessi coinvolti, secondo una *ratio* imperniata sulla flessibilità.
I codici potrebbero, infatti, intervenire per tracciare "l'organigramma" dei soggetti interessati, identificando chi è destinatario degli interventi e di quali diritti specifici sia portatore in ragione dei differenti *output* prodotti. Ciò consentirebbe di definire anche chi è titolare di obblighi, in quanto utilizzatore di sistemi di IA, e le tutele da applicare alla singola casistica.

---

578 Il paragrafo 3 dell'art. 69 della proposta di Regolamento IA prevede ora che "*i codici di condotta possono essere elaborati da singoli fornitori di sistemi di IA o da organizzazioni che li rappresentano o da entrambi, anche con la partecipazione degli utenti e di tutti gli altri portatori di interessi, compresi i ricercatori scientifici, e delle loro organizzazioni rappresentative, in particolare i sindacati, e delle organizzazioni dei consumatori. I codici di condotta possono riguardare uno o più sistemi di IA tenendo conto della similarità della finalità prevista dei sistemi pertinenti. I fornitori che adottano codici di condotta designano almeno una persona fisica responsabile del monitoraggio interno*".

579 Lo "*United Nations sustainable development cooperation framework*", pubblicato il 3.6.2019, descrive *Human Rights Approach* come "*the Human Rights-Based Approach to Development is a conceptual framework for the process of sustainable development that is normatively based on international human rights standards and principles and operationally directed to promoting and protecting human rights. Under the HRBA, the plans, policies and processes of development are anchored in a system of rights and corresponding obligations established by international law, including all civil, cultural, economic, political and social rights, and the right to development. HRBA requires human rights principles (equality and nondiscrimination, participation, accountability) to guide UN development cooperation, and focus on capacity development of both 'duty-bearers' to meet their obligations and 'rights-holders' to claim their rights*" (par. 19). Lo stesso documento prevede la necessità di applicare lo HRBA anche al trattamento dei dati personali "*the UN CCA will analyse existing data and data gaps for national SDG indicators. It should go beyond official national statistics to use new sources of data and diagnostic tools, including but not limited to big data, national surveys and assessments, targeted surveys using mobile technology and others. This should be done in accordance with the human rights-based approach to data, international data protection standards and the UN Principles on Personal Data Protection and Privacy*" (par. 36).

Il processo di redazione di un Codice di condotta dovrebbe, quindi, analizzare *in primis* le funzioni a cui è abilitato il sistema di IA, le finalità per cui viene adoperato, i dati acquisibili e gli *output* elaborabili.
Sulla base di queste informazioni, il Codice potrebbe, inoltre, disciplinare tempi e modalità di redazione e aggiornamento della Valutazione di Impatto[580] finalizzata a comprendere i rischi e gli effetti del funzionamento dei sistemi.
Da ultimo, potrebbe essere predisposto un sistema di monitoraggio e di impugnazione che risulti sicuro e agevole in ragione degli interventi umani previsti e della certezza delle informazioni condivise.
Tutte le scelte compiute nella singola realtà aziendale, dalla progettazione al monitoraggio del sistema, andrebbero così trasposte nei Codici di condotta in modo da individuare prassi tecniche, organizzative e giuridiche flessibili e aderenti alle contingenze dei lavoratori.

4.4. La centralità della persona del lavoratore garantita da un approccio antropocentrico e dalla sorveglianza umana

La tutela dei lavoratori, informata alla trasparenza dei nuovi poteri datoriali, deve tenere in considerazione anche le garanzie a questa fornite dal principio personalista[581] che suggerisce un approccio antropocentrico[582] e la conseguente garanzia di ricevere una sorveglianza umana.
Nella normativa italiana[583] ed europea[584] si ha un ricorrente riferimento alla sorveglianza umana della macchina, posta quale elemento fondante alla formazione di persone informate sui nuovi sistemi di Intelligenza Artificiale.

L'Accordo quadro sulla digitalizzazione[585], finalizzato a sostenere il successo della trasformazione digitale dell'economia europea e a gestire le sue ripercussioni sul mercato del lavoro, ha sottolineato la rilevanza che deve essere attribuita alle tutele abilitate da una sorveglianza umana.

La proposta di Regolamento sulla Intelligenza Artificiale compie un ulteriore passo in avanti in questa direzione e specifica che i sistemi di Intelligenza Artificiale devono essere progettati in modo da poter essere efficacemente monitorati da persone fisiche per prevenire o ridurre al minimo i rischi derivanti dal loro uso.

---

580 L'analisi dei rischi dovrebbe contemplare le funzioni non solo previste, ma prevedibili, definendo le ipotetiche strategie da adottare a tutela degli interessati.
Sulla base delle risultanze di tale valutazione sarebbe, così, possibile definire interventi tecnici ed organizzativi che consentano di tutelare i diritti e identificare i doveri dei diversi soggetti coinvolti.

581 Il principio personalista è uno dei principi fondamentali della Costituzione e sottolinea il rispetto e la tutela della dignità umana, dei diritti inalienabili della persona e dei valori che derivano dalla stessa. I riferimenti al principio personalista si possono rinvenire negli articoli 2 (che fa riferimento ai diritti inviolabili dell'individuo), nell' articolo 3 (il quale sviluppa il principio di uguaglianza), nell'art. 13 (attinente alle libertà personali) e nell'art. 32 (inerente al diritto alla salute e protegge la libertà e la dignità della persona in relazione alle decisioni assunte in tale ambito).

582 L'indicazione di un approccio antropocentrico era già stato indicato dalla Commissione europea nella comunicazione del 25 aprile 2018 ""*Strategia per l'I.A*" (COM(2018) 237 fina). Successivamente, su *input* del Consiglio europeo sono stati elaborati sette specifici requisiti per creare una IA affidabile e specificatamente: intervento e sorveglianza umani, robustezza tecnica e sicurezza, riservatezza e *governance* dei dati, trasparenza, diversità, non discriminazione ed equità, benessere sociale e ambientale, *accountability*. Tali criteri sono stati successivamente accolti nella comunicazione della Commissione "Creare fiducia nell'intelligenza artificiale antropocentrica" COM(2019) 168 final.

583 Art. 4 Statuto dei Lavoratori.

584 Art. 22 comma 3 GDPR, proposta di Regolamento su IA.

585 *European social partners framework agreement on digitalization* del 22 giugno 2020. In merito Senatori, I., *The European Framework Agreement on Digitalisation: a Whiter Shade of Pale*?, in *Italian Labour Law e-Journal*, 13(2), 2020, pp. 159–175; Rota, A., *Sull'Accordo quadro europeo in tema di digitalizzazione del lavoro*, in *Labour & Law Issues (LLI)*,vol. 6, n. 2, 2020, pp.C.23-C.48.

L'obiettivo della sorveglianza umana sarà, come stabilito dall'articolo 14 della proposta, quello di prevenire o eludere i rischi per la salute, la sicurezza o i diritti fondamentali dei lavoratori che possono sorgere con l'impiego di sistemi di IA ad alto rischio.
Le misure adottate in tema di sorveglianza umana permettono, infatti, di poter comprendere appieno le capacità e i limiti dei sistemi di Intelligenza Artificiale e di monitorare adeguatamente il suo funzionamento. Permettono, inoltre, di comprendere le tendenze del sistema a far affidamento, in maniera automatica o sproporzionata, alle informazioni elaborate dal medesimo sistema di IA.

Il diritto di sorveglianza umana dell'algoritmo determina, così, due limitazioni al funzionamento automatico dei sistemi di IA.
La prima fa riferimento ad un rifiuto di un totale meccanicismo dei poteri datoriali, ponendo quale centrale un approccio antropocentrico in un contesto che tende a sfuggire al controllo umano.
Ratio a cui si ispira anche l'art. 4 SL la cui finalità è quella di tutelare "*la dimensione personalistica, l'intenzione di tutelare la privatezza del lavoratore di fronte all'occhio scrutatore e onnipresente di un Grande Fratello aziendale*"[586].
In secondo luogo, il concetto di sorveglianza umana rinvia a quello di revisione della decisione assunta dalla macchina[587].
Il singolo lavoratore deve, quindi, poter manifestare una propria autonomia d'azione nei confronti di un sistema automatizzato sia per richiedere una spiegazione comprensibile sia per ottenere un riesame.
Ciò determina la possibilità di poter conoscere quali dati siano stati acquisiti ed elaborati e di poterli estrapolare dal sistema. Meccanismo inverso rispetto a quello generale di funzionamento dei sistemi algoritmici e di IA in cui i dati vengono accorpati e correlati.

La garanzia della sorveglianza umana comporta l'insorgere di una corrispondente responsabilità datoriale che assicuri un approccio *human-in-command*, la cui *ratio* di salvaguardia si può ritrovare anche in altre due norme che condividono con AIR l'elemento della valutazione e gestione del rischio.
Si tratta dell'art. 35 del GDPR, inerente alla valutazione d'impatto per il trattamento dei dati personali e dell'art. 28 del D. Lgs. 81/2008 in materia di salute e sicurezza sul lavoro.
Tali autonomi obblighi vigenti in capo al datore di lavoro portano ad una responsabilizzazione dello stesso in riferimento alla protezione di diritti fondamentali dei lavoratori e un conseguente dovere di conformità alla normativa.
Parimenti, la garanzia di una sorveglianza umana determina l'insorgere di un obbligo in capo al datore di lavoro di valutare e gestire i rischi dei lavoratori collegati all'uso di sistemi di IA[588].

Resta, in ogni caso, da definire quale sia la portata che può avere l'intervento umano nel processo di sorveglianza e in quale fase debba intervenire.

---

586 D'Antona M., *L'art. 4 dello Statuto dei Lavoratori ed elaborati elettronici*, in De Luca-Tamajo R., Imperiali-D'Afflitto R., Pisani. C., Romei R. (a cura di), *Nuove tecnologie e tutela della riservatezza del lavoratore*, Giuffrè Editore, Milano, 1988, pp. 204-205.
Come si legge nella Relazione governativa al d.d.l. sullo Statuto dei Lavoratori "*il divieto di utilizzazione di mezzi di controllo a distanza (…) parte dal presupposto che la vigilanza sul lavoro, ancorché necessaria nell'organizzazione produttiva, vada mantenuta in una dimensione "umana", e cioè non esasperata dall'uso di tecnologie che possono rendere la vigilanza stessa continua e anelastica, eliminando ogni zona di riservatezza e di autonomia nello svolgimento del lavoro*".
587 Riprendendo i commenti della dottrina sulla ratio dell'art. 4 SL "*Una cosa è il controllo del sorvegliante, che interviene, contesta direttamente un'infrazione, dà modo al lavoratore di difendersi, di prospettare le sue ragioni; altra cosa è il controllo anonimo, odioso, spinto fino all'esasperazione, da parte di un meccanismo controllato soltanto dalla direzione"*. Smuraglia C., *Progresso tecnico e tutela della personalità del lavoratore*, in *Rivista Giuridica del Lavoro*, Vol. 1, 1960, p. 312.
588 In merito si rinvia alle riflessioni offerte da Marco Peruzzi in Peruzzi M., *Intelligenza Artificiale e lavoro. Uno studio su poteri datoriali e tecniche di tutela*, Giappichelli Editore, Torino, 2023, pp. 164 ss.

La sorveglianza umana può, infatti, svilupparsi in diversi momenti di operatività del sistema di Intelligenza Artificiale.
L'intervento umano potrebbe porsi *ex ante* o *in itinere* al processo algoritmico, oppure intervenire *ex post* come diritto al riesame o di valutazione della decisione assunta.
Ulteriore aspetto da considerare oltre alla fase di intervento è anche la sua frequenza.
La sorveglianza umana potrebbe, infatti, essere richiesta in modo alternativo solo in alcuni momenti, oppure risultare intrinseca ad ogni fase di operatività della macchina.

La definizione di tali aspetti, in quanto elemento proprio della progettazione e programmazione dei sistemi, potrebbe rientrare tra gli ambiti rimessi a una partecipazione collettiva dei lavoratori, al fine di pianificare i differenti passaggi e i momenti di contraddittorio necessario con un operatore umano.
Tali aspetti sono stati, per esempio, oggetto di una prima contrattazione collettiva in Spagna ove il XXIV *Convenio colectivo* del settore bancario all'articolo 80, comma 5 precisa espressamente che il crescente sviluppo del contributo della tecnologia richiede un'attenta implementazione quando esso viene applicato al campo della persona. Per tale ragione stabilisce che "*i lavoratori hanno il diritto di non essere oggetto di decisioni basate solo ed esclusivamente su variabili automatizzate, tranne nei casi previsti dalla legge, così come il diritto alla non discriminazione in relazione alla decisione e ai processi quando entrambi sono basati esclusivamente su algoritmi, potendo richiedere, in questi casi, il ricorso e l'intervento delle persone indicate a tal fine dalla società in caso di discrepanze*"[589].

Anche se le evidenze di un tale intervento risultano ancora sporadiche, la circostanza che la contrattazione collettiva inizi a interessarsi di questi aspetti è manifestazione di un indubbio segno dell'importanza sottesa alla questione.

4.5. Individuazione di soggetti designati competenti in materia quali esperti che coadiuvino i lavoratori nella comprensione dei sistemi

Le tutele volte a favorire la trasparenza dei sistemi possono, inoltre, prendere in considerazione l'individuazione di soggetti competenti in materia e, perciò, designati a ricevere le informazioni e a valutare i rischi connessi all'uso delle nuove tecnologie.
L'impiego di strumenti di analisi ed elaborazione dei dati può comportare l'emersione di nuovi rischi che possono essere rilevanti a livello individuale e collettivo.
L'approccio basato sul rischio costituisce un principio centrale del sistema di garanzie applicabile alla protezione dei dati, sviluppato nel GDPR e ripreso dalla proposta di Regolamento sull'Intelligenza Artificiale[590].
La proposta di Regolamento sull'Intelligenza Artificiale prevede, infatti, un processo di gestione del rischio che coinvolge l'intero ciclo di vita del sistema di IA, richiedendo aggiornamenti sistematici e regolari al fine di determinare le misure di gestione più appropriate[591].

L'approccio basato sul rischio è centrale anche nelle tutele afferenti alla salute e sicurezza dei lavoratori.
In merito, l'impiego di sistemi di IA in ambito lavorativo genera due profili di interesse.
In primo luogo, la qualificazione dei sistemi di IA come sistemi ad alto rischio impatta sugli adempimenti a cui è tenuto il datore di lavoro in materia di salute e sicurezza e, conseguentemente, sulla redazione del DVR e sugli obblighi di formazione e consultazione in materia.

589 Traduzione dell'autrice.
590 Cfr. art. 11 proposta di Regolamento IA.
591 Cfr. art. 9 proposta di Regolamento IA.

In secondo luogo, la qualifica di rischio elevato attribuita all'IA interferisce anche sul rispetto del principio di precauzione, su cui è imperniato il TU del 2008, in riferimento ai pericoli connessi all'uso di apparecchiature tecnologiche.

Il richiamo al concetto di rischio nell'ambito della salute e sicurezza dei lavoratori e ai doveri di informazione che incombono sul datore di lavoro potrebbe fungere da criterio orientativo in merito ai diritti informativi sui sistemi di monitoraggio informatico e al riconoscimento degli stessi quale tutela individuale o collettiva.
Al pari di quanto previsto in ambito di salute e sicurezza dei lavoratori potrebbe, infatti, essere individuato un soggetto che funga da rappresentante dei lavoratori[592]. Questo, pur essendo una figura individuale, agirebbe da rappresentante della collettività e, in quanto tale, preposto a esercitare il diritto di informazione e a ricevere le istruzioni relative all'uso dei sistemi algoritmici o di IA.

Tale ipotesi richiederebbe, pertanto, una formazione specifica al pari di come è stato ipotizzato da parte della dottrina in materia di *privacy*. In questo caso il soggetto designato fungerebbe da "*anello di collegamento tra i lavoratori interessati dai trattamenti e il vertice dell'organizzazione aziendale che predispone le misure atte ad umanizzare la tecnologia e a renderla rispettosa dei diritti*"[593].
La previsione di un soggetto esperto che coadiuvi i lavoratori nella comprensione dei sistemi automatizzati deve essere accolta favorevolmente anche nel caso in cui questi siano rappresentati da un organismo esponenziale la cui presenza potrebbe risultare poco incisiva ove le conoscenze (e competenze) in ambito informatico risultino insufficienti per tutelare gli interessi dei prestatori.
In questo senso, deve essere citata positivamente la previsione introdotta della proposta di Direttiva sul lavoro mediante piattaforme digitali ove prevede all'art. 9 la possibilità non solo per i singoli lavoratori, ma anche per i loro rappresentanti, di essere "*assistiti da un esperto di loro scelta nella misura in cui ciò sia loro necessario per esaminare la questione oggetto di informazione e consultazione e formulare un parere*"[594].

Un'effettiva e più approfondita comprensione dei sistemi algoritmici e di IA mediata – ove necessario - dall'intervento di esperti in materia risulterebbe, quindi, un espediente volto a favorire un confronto realmente "informato" e, dunque, equilibrato tra le parti.

---

[592] Il suggerimento volto al legislatore *de iure condendo* di introdurre una figura *ad hoc* eletta dai dipendenti per tutelarne la *privacy*, in maniera analoga a quanto avviene con il rappresentante dei lavoratori per la sicurezza di cui al D.Lgs n. 81/2008 è stata formulata da Orietta Dessì. In merito Dessì O., *Il controllo a distanza sui lavoratori. Il nuovo art. 4 Stat. lav.,* Edizioni Scientifiche Italiane, Napoli, 2017, pp. 175-177. Conformemente Ingrao A., *Data-driven management e strategie collettive di coinvolgimento dei lavoratori per la tutela della privacy*, in *Labour & Law Issues* (LLI), vol. 5, n. 2, 2019, pp. 140-141; Sartori A., *Il controllo tecnologico sui lavoratori. La nuova disciplina italiana tra vincoli sovranazionali e modelli comparati*, G. Giappichelli Editore, Torino, 2020, p. 336.
[593] Ingrao A., *Controllo a distanza e privacy del lavoratore alla luce dei principi di finalità e proporzionalità della sorveglianza*, in *Labour & Law Issues (LLI),* vol. 9, n. 1, 2023, p. I 119. Nel medesimo senso di "*anello di collegamento tra i lavoratori interessati dai trattamenti e il vertice dell'organizzazione aziendale*" Ingrao A., *Data-Driven management e strategie collettive di coinvolgimento dei lavoratori per la tutela della privacy*, in *Labour & Law Issues (LLI)*, 2, 2019, p. 128. L'autrice ipotizza la creazione di un rappresentante dei lavoratori per la *privacy* (RLP) la cui attività risulterebbe di supporto sia ai lavoratori che al titolare del trattamento al fine di dimostrare la propria *compliance* al GDPR. In merito anche Zilli A., *La trasparenza nel lavoro subordinato. Principi e tecniche di tutela*, Pacini Giuridica, 2022, p. 66, Libro in Open Access scaricabile gratuitamente dall'archivio IRIS – Anagrafe della ricerca https://air.uniud.it/.
[594] Art. 9 paragrafo 3 proposta di Direttiva.

4.6. Pulizia dei dati per garantire la qualità dei *data set* impiegati

Le garanzie dei lavoratori devono, infine, tenere in considerazione la qualità dei *data set* impiegati dagli strumenti digitali.

La tutela della trasparenza, in contrapposizione con l'opacità del processo decisionale datoriale, passa anche attraverso la pulizia dei dati integrati nei *data set*.

Come si ha avuto modo di approfondire nel terzo capitolo, a cui si rimanda, le criticità[595] connesse ad un data set viziato impiegato per addestrare un sistema algoritmico o di IA, portano alla generazione di *bias* - da cui possono discendere distorsioni o discriminazioni- , nonché fenomeni di alterata rappresentazione della realtà osservata con manifestazioni di *underfittin*[596]*g* o, al contrario, di *overfitting*[597].

L'accessibilità e la comprensione dei *data set* adoperati è, dunque, un passaggio necessario per verificare la qualità delle informazioni adottate.

Il maggior impiego di dati può, infatti, favorirne l'elaborazione e aumentare la probabilità di un risultato rilevante e attinente alle finalità di trattamento richieste.

Contestualmente, però, diviene sempre più sfuggente il controllo delle qualità dei dati di ingresso che divengono un fattore strategico delle decisioni elaborate.

Il rischio che ne consegue è quello di analizzare dati "sporchi"[598], ossia fuorvianti o non attinenti agli scopi prefissati, caratteristica riscontrabile più facilmente ove i dati acquisiti siano "non autoevidenti" e, pertanto, maggiormente condizionabili dall'elaborazione.

Uno dei problemi connessi alla datificazione del lavoro è, dunque, quello di interpretare e selezionare i dati realmente rilevanti tra tutti quelli prodotti dai lavoratori digitali.

Possedere molti dati non si traduce automaticamente nell'accesso a molte informazioni validamente spendibili.

Da ciò la necessità di affinare le tecniche di "*data cleaning*", da intendersi quale processo di identificazione, correlazione e rimozione di incongruenze che consente di garantire l'affidabilità dei dati.

La pulizia dei dati integrati in un *data set* risulta, quindi, un'attività iterativa che richiede la combinazione di conoscenze tecniche e un'approfondita comprensione del dominio di riferimento.

Quando si parla, dunque, di qualità del dato bisogna tenere in considerazione non solo la natura di questo, ma anche la fonte da cui esso proviene, nonché le finalità che si intendono raggiungere con il suo utilizzo.

In relazione alla provenienza, l'acquisizione di dati da ambienti lavorativi digitali potrebbe fungere da elemento di controllo essendo un ambito di osservazione che può essere definito "chiuso", anche se alimentato da informazioni eterogene e non strutturate.

I dati dei lavoratori costituiscono, infatti, un dominio applicativo[599] delimitato nonostante sia generato da dati ottenuti da plurime fonti rappresentate dai differenti strumenti digitali.

---

595 In merito anche Peruzzi M., *Intelligenza Artificiale e lavoro. Uno studio su poteri datoriali e tecniche di tutela*, Giappichelli Editore, Torino, 2023, p. 152.

596 Ovvero di sottorappresentazione degli scenari di interesse.

597 Ossia di sbilanciamento per eccedenza di una classe di elementi rispetto ad altri.

598 I dati presenti in sistemi impiegati per gestire il personale, come HRIS sono complessi, molto spesso inutili e spesso qualificabili some particolari, oltre che personali. In merito al tipo di analisi che possono essere compiute e alle preliminari operazioni di pulizia si rinvia allo studio compiuto da Shahin Manafi Varkiani, Francesco Pattarin, Tommaso Fabbri e Gualtiero Fantoni ove si analizzano le tecniche di *machine learning* su un *set* di dati reali di una grande società finanziaria italiana al fine di analizzare il turnover dei dipendenti e la previsione del grado di abbandono. Manafi Varkiani S., Pattarin F., Fabbri T., Fantoni G., *Predicting Employee Attrition by Machine Learning*, Conference Paper, Conference: 2021 4th International Conference on Artificial Intelligence and Big Data (ICAIBD), May 2021.

599 Per dominio applicativo nel contest informatico e dello sviluppo dei software ci si riferisce a una categoria o a un ambito specifico di applicazioni che condividono caratteristiche o funzionalità simili. Un dominio applicativo rappresenta, dunque, un'area di interesse o un settore in cui un determinato tipo di *software* viene utilizzato per risolvere problemi o fornire servizi specifici.

La precisa definizione del dominio comporta anche un'approfondita conoscenza delle problematiche che si intendono risolvere, ovvero delle finalità che si intendono raggiungere per garantire la robustezza e l'attendibilità del *data set* impiegato.
Ciò in accordo con quanto previsto del GDPR in riferimento alle "*finalità del trattamento*"[600] quale principio fondante alla raccolta e utilizzo dei dati.

L'applicazione del principio di trasparenza ai *data set* deve, così, condurre a operazioni preliminari alla loro creazione e utilizzo.
Una migliore "*performance* dei dati" può portare, dunque, ad un maggior grado di tutela dei lavoratori.
La creazione di *data base* sempre più precisi, realistici e affidabili deve intrecciarsi con la creazione di buone prassi, così da costituire un substrato con cui dar vita (anche mediante Intelligenza Artificiale) a modelli che definiscano strategie efficaci e utili al mondo del lavoro quali l'innalzamento degli *standard* di benessere psicofisico e di sicurezza sul lavoro.
Un tale approccio può, inoltre, favorire il mercato delle competenze (*skills*) e la creazione di pacchetti formativi personalizzati, calibrati sulle attitudini dei singoli lavoratori e rapportati alle esigenze datoriali.

Per giungere a una reale trasparenza e comprensibilità del procedimento di elaborazione e dei *data set* impiegati appare, quindi, imprescindibile compiere una preliminare "significazione" degli stessi al fine di appurare quali dati, o loro correlazione, possano produrre effetti giuridici.
La comprensione di quali dati possano tradursi in informazioni pertinenti, tempestive e utilizzabili consente, al contempo, di identificare quelli che sono potenzialmente pregiudizievoli delle libertà dei lavoratori.
Ciò può garantire l'esercizio delle tutele vigenti o costruirne di nuove, come nel caso di quelle collettive, tralasciando di definire lo strumento da cui vengono tratte le informazioni.
In tale maniera, potrebbe essere abbandonata la ricerca di una definizione autentica di "strumento di lavoro", distinta da quella di "strumento di controllo", prendendo coscienza del fatto che tutti i dispositivi informatici hanno *in re ipsa* la potenzialità di monitoraggio.

In riferimento a quanto esposto si possono citare ad esempio alcuni studi che stanno operando in tale direzione.
Alcune ricerche, infatti, tentano di interpretare i dati, identificando quelli necessari per ottenere *insight* sulle risorse umane.
Il fine è quello analizzare i flussi di dati generati dai dipendenti negli ambienti digitali e correlarli ai risultati dei sondaggi somministrati. Il nesso tra comportamenti digitali e *survey* cerca, dunque, di attribuire un significato ai dati registrati.
Tale analisi è stata compiuta dall'Università di Modena e Reggio Emilia[601] che ha raccolto i dati riferiti ad un campione di 107 dipendenti adibiti a una *business unit* di un'azienda internazionale di vendita al dettaglio di beni. Lo studio, condotto per la durata di due anni, ha correlato numero e tipo di *file*, prodotti dai dipendenti sulla piattaforma collaborativa, agli atteggiamenti rilevati contestualmente nei sondaggi.

[600] Art. 5 lett. b) del GDPR.
[601] Fabbri T., Mandreoli F., Martoglia R., Scapolan A. C., *Employee Attitudes and (Digital) Collaboration Data: A Preliminary Analysis in the HRM Field*, 28th International Conference on Computer Communication and Networks (ICCCN), n. 07 2019, pp.1-6. This work is supported by UniMoRe under the project "*Framing employee attitudes and digital work behaviors to support data-driven human resource management*".

La ricerca ha consentito di giungere ad alcune interpretazioni trovando, per esempio, una correlazione tra interazioni compiute sulla piattaforma e l'integrazione dei dipendenti con l'organizzazione o l'adattamento alla mansione svolta.

Attribuire un significato ai dati permette, inoltre, di contribuire allo sviluppo dell'*explainable* AI (xAI)[602], ovvero di quel sistema di Intelligenza Artificiale in grado di rendere intellegibile e motivata una decisione, permettendo l'accesso e la partecipazione dei destinatari al processo valutativo.
Lo sviluppo dell'automazione in forme più complesse e autosufficienti genera parallelamente la necessità di comprendere come vengono prese le decisioni al fine di giudicarne la correttezza.
L'*explainable* AI affronta la problematica, ponendosi l'obiettivo di progettare un'Intelligenza Artificiale comprensibile dagli utilizzatori, rendendone accessibili i processi.
La comprensione dei procedimenti di automazione potrà consentire di informare gli interessati in merito a quali dati siano stati acquisiti, per quali finalità siano stati impiegati e in base a quali regole.

602 Una definizione è stata fornita da Gunning che l'ha descritta come "*XAI will create a suite of machine learning techniques that enables human users to understand, appropriately trust, and effectively manage the emerging generation of artificially intelligent partners"*. Gunning D., *Explainable artificial intelligence (xAI)*, in *Technical Report, Defense Advanced Research Projects Agency* (DARPA), 2017, pp. 44 ss.

Note conclusive e proposte per l'attuazione delle tutele di nuova generazione

La disamina fin qui compiuta ha avuto per obiettivo la definizione delle modalità in cui si manifesta il potere di controllo tecnologico su prestazioni "native digitali" e di individuare i profili di continuità o discontinuità con il controllo esercitato su prestazioni analogiche.
L'analisi svolta suggerisce alcune considerazioni conclusive in relazione al (nuovo) modo di manifestarsi del potere di controllo e ai limiti che allo stesso è opportuno vengano apposti.

Un primo aspetto riguarda lo sviluppo del potere di controllo nella nuova forma di "poter di controllo direttivo"[603].
Trasformazione che deriva dall'impiego di strumenti tecnologici per gestire le attività dei lavoratori (come *HRIS)* o ne consentono la prestazione digitale (come le *Digital Workplace*).
Tale potere fonda la propria origine nella capacità degli strumenti computazionali di accedere ed elaborare grandi quantità di dati dei lavoratori, acquisiti durante l'esecuzione delle loro prestazioni, e di monitorarne in modo dettagliato e continuo non solo gli spetti professionali, ma anche quelli personali.
Grazie alla tecnologia il datore di lavoro può ora dedurre specifiche caratteristiche dei prestatori – anche estranee all'attività lavorativa - sulla base di dati non immediatamente correlati a tali peculiarità.
Potenzialità che risultano particolarmente insidiose quado i dati analizzati sono "non autoevidenti", ovvero non immediatamente autoesplicativi e richiedono una necessaria interpretazione che ne riveli il significato.
Il potere di "controllo direttivo" si riferisce, dunque, alla capacità dei datori di lavoro di esercitare un controllo diretto e dettagliato sulle attività e caratteristiche dei lavoratori e, al contempo, di prendere decisioni sulla base delle informazioni dedotte con l'elaborazione dei dati.
Tendenza che *"risulta sensibilmente avvalorata dall'impostazione adottata nella proposta di direttiva sul lavoro tramite piattaforma, che esalta il ruolo del controllo (anche) come veicolo di direzione e organizzazione del lavoro altrui"*[604].
Il potere di controllo si dota, così, di nuove capacità grazie alla tecnologia computazionale, modificando la propria natura e superando la tradizionale divisione tra poteri datoriali.
Il potere di controllo, trasformato in "controllo sui dati", consente in tal modo al datore di lavoro una sorveglianza capziosa, permettendo di monitorare e, contestualmente, di amministrare le informazioni acquisite sui lavoratori.
Le riflessioni sul potere di controllo si intrecciano, dunque, inevitabilmente con la disciplina dei dati personali, in quanto la nuova forza riconosciuta al potere di controllo giunge dal dominio sugli stessi.
Il potere di "controllo direttivo" trova, infatti, fondamento nell'acquisizione e, soprattutto, nell'elaborazione dei dati da cui è possibile trarre nuove informazioni.

Un secondo aspetto interessa la forza del "potere di controllo direttivo", generato dalla tecnologia sui dati, che trova fondamento nell'opacità del proprio manifestarsi.
Questa opacità può derivare dalla complessità dei sistemi algoritmici o di IA utilizzati, dalla mancata trasparenza nelle modalità di raccolta e trattamento dei dati, nonché dalla difficoltà per i lavoratori di comprendere come vengono sfruttate le informazioni.

---

603 In merito Tebano L, *Lavoro, potere direttivo e trasformazioni organizzative,* Editoriale Scientifica, Napoli, 2020; Tebano L*., La digitalizzazione del lavoro tra intelligenza artificiale e gestione algoritmica*, in *IANUS*, n. 24, 2021, pp. 43 ss.; Tebano L, *Fabbrica 4.0 e potere di "controllo direttivo"*, in Rusciano M., Gaeta L., Zoppoli L. (a cura di), *Mezzo secolo dallo statuto dei lavoratori*, in *Quaderni della Rivista Diritti Lavori Mercanti*, n. 8, 2020, pp. 443 ss.
604 Tebano L*., La digitalizzazione del lavoro tra intelligenza artificiale e gestione algoritmica*, in *IANUS*, n. 24, 2021, p. 49. In riferimento alle piattaforme digitali Laura Tebano osserva che in tale contesto l'ibridazione dei poteri datoriali arriva a ricoprire anche il potere disciplinare.

L'opacità del potere di controllo può giungere anche dalla tipologia di dati acquisiti che, ove "non autoevidenti", possono celare - dietro un'apparente neutralità - una pluralità di informazioni significative.
In tale ipotesi, ove la ponderazione sulla legittimità di eseguire un controllo dei prestatori venga compiuta a priori su dati non significativi, il giudizio eseguito *ex ante* può risultare fallace.
Conseguentemente, se i lavoratori ignorano come avvenga la raccolta e l'elaborazione dei dati o non sono in grado di comprendere le informazioni fornite a riguardo, i datori di lavoro possono sfruttare tale *vulnus* per esercitare un controllo eccessivo (in quanto svincolato da ogni limite) e disumano (ovvero integralmente delegato alla macchina)[605].
Diretta conseguenza di ciò è non solo la violazione della libertà di autodeterminazione informativa dei lavoratori, ma anche l'inconsapevole soggezione degli stessi a trattamenti arbitrari o discriminatori.

Il binomio "dati-potere datoriale" pone, così, nuovi interrogativi alle tutele offerte dal diritto.
La terza riflessione interessa, pertanto, i limiti che possono essere apposti al nuovo "potere di controllo direttivo".
Le esigenze di tutela dei lavoratori che emergono dalla ricerca compiuta non permettono di tracciare una soluzione certa e immutabile, dato l'inarrestabile sviluppo della tecnologia.
Le strategie devono adattarsi al cambiamento tenendo, però, sempre presente i principi posti a fondamento delle tutele, i quali devono essere recuperati e applicati.
Se, dunque, il potere di "controllo direttivo" trae la propria forza dall'opacità con cui vengono trattati i dati, appare necessario contrappore una serie di interventi che rendano trasparenti le azioni compiute.
Il principio di trasparenza può, dunque, contrastare l'intensità del potere di controllo - rendendolo palese nel suo manifestarsi - e ricoprendo un ruolo abilitante dei diritti dei lavoratori: la conoscenza è il presupposto per attivare la salvaguardia degli interessati.

L'ultimo capitolo della ricerca ha, dunque, analizzato le soluzioni proposte dalle norme europee di prossima emanazione e suggerito alcune strategie di intervento per una efficace esecuzione del diritto di informazione.
Nel testo si è posta attenzione alla dimensione superindividuale del principio di trasparenza, individuando nella partecipazione collettiva dei lavoratori una possibile contromisura al potere datoriale.

Il divieto di un monitoraggio diretto e continuativo dell'attività lavorativa trova, infatti, al momento una tutela ripartita secondo un sistema "dualistico", fondato su interventi individuali e collettivi.
In particolare, ove la forza del controllo datoriale derivi dall'accesso ai dati e alle informazioni da questi desumibili, deve potersi contrappore un egual potere che ne limiti gli abusi favorendo l'intellegibilità dei sistemi.
Bilanciamento che può risultare inefficacie ove l'azione di contrasto sia rimessa ai singoli prestatori.

Il coinvolgimento dei lavoratori nella salvaguardia dei dati e il loro intervento anche su aspetti programmatici (come la pianificazione condivisa in merito all'introduzione di tecnologie digitali in contesti lavorativi), può garantire una tutela più efficiente e sicura, agevolando una migliore comprensione delle informazioni fornite.

[605] La questione viene sollevata anche da Marco Peruzzi, il quale osserva che l'utilizzo di sistemi di intelligenza artificiale da parte del datore di lavoro può addurre principalmente a due problematiche: da un lato l'aumento del rischio di violazioni dei diritti di conosciuti al lavoratore, dall'altro la difficile individuazione e dimostrazione di detta violazione. In merito si rinvia Peruzzi M., *Intelligenza Artificiale e lavoro. Uno studio su poteri datoriali e tecniche di tutela*, Giappichelli Editore, Torino, 2023, pp. 7 ss.

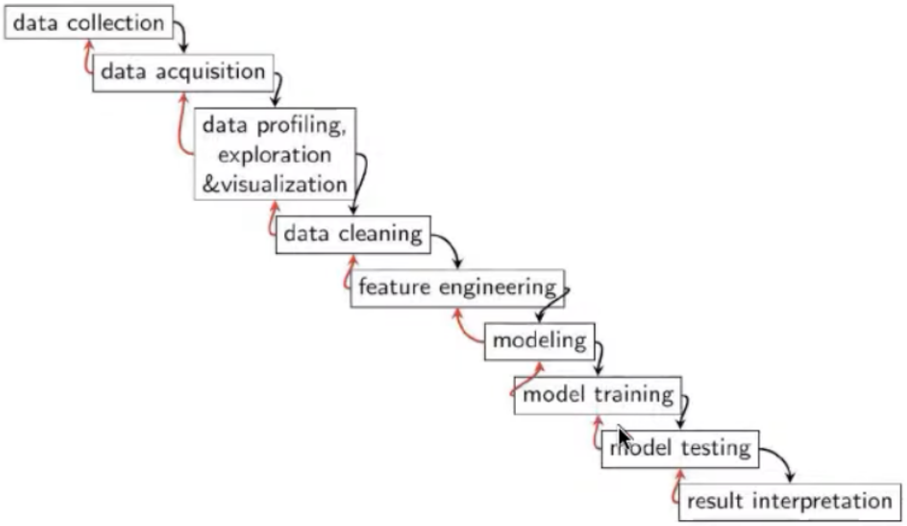
La partecipazione dei lavoratori può, così, garantire un maggior grado di trasparenza, facilitando la consapevolezza dei processi compiuti e procedimentalizzando il potere di controllo datoriale attraverso la definizione di momenti di verifica.
La garanzia della trasparenza nel contesto dell'organizzazione digitale investe direttamente la tutela della dignità del lavoratore in quanto consente di invertire lo *status* del prestatore da soggetto passivo "*dell'informazione, di datazione, di profilazione*" a soggetto attivo "*detentore dell'informazione*"[606].
Il coinvolgimento attivo dei lavoratori può, inoltre, favorire soluzioni flessibili che permettano di adattare tempestivamente tutele specifiche calate sulle singole realtà lavorative, favorendo un equilibrio tra prerogative datoriali e diritti dei prestatori.
L'opzione, dunque, di delegare anche a strumenti di "*soft law"* (come i Codici di condotta) la definizione dei singoli interventi, appare una scelta correlata all'incessante sviluppo della tecnologia.

Un'ulteriore valutazione riguarda la distinzione, tuttora centrale, sulla natura degli strumenti e l'eventuale possibilità di definire alcuni dispositivi tecnologici quali "meri strumenti di lavoro", nonostante la loro connaturata capacità di acquisire dati.
Tale distinzione si fonderebbe sulle caratteristiche dei dispositivi, distinguendo tra strumenti che eseguono un semplice monitoraggio, da quelli che compiono un vero e proprio controllo tracciando la prestazione.
L'esigenza nasce dalla considerazione che i nuovi congegni digitali pongono - inevitabilmente - il datore di lavoro nella possibilità di "vedere" (ovvero di "monitorare") tutti i dati dei lavoratori, ma di esercitare il potere di controllo solo ove questi siano comprensibili.
Ci si domanda, quindi, se e in che misura i dispositivi digitali possano rientrare nella definizione di "strumenti di lavoro", di cui al secondo comma dell'art. 4 SL, e porsi così al di fuori dei vincoli posti dalla norma statutaria.

Una soluzione potrebbe essere rintracciata non tanto nella qualifica dello strumento, ma in quella delle sue funzionalità, distinte in "monitoraggio" e "controllo", considerando il primo come una mera raccolta e osservazione di dati e il secondo come l'esercizio di un potere decisionale o coercitivo.
Distinzione possibile solo nel caso di dati definiti come "non autoevidenti".
La ripartizione porterebbe a considerare l'attività di monitoraggio (intrinseca a tutti gli strumenti tecnologici) come di mera osservazione di dati "non autoevidenti" qualora questi non vengano resi intellegibili con l'elaborazione. In tale ipotesi, l'osservazione preliminare ad una loro analisi si porrebbe al di fuori dell'ambito del potere di controllo datoriale.
Diversamente, il potere di controllo verrebbe a sussistere solo ove i dati siano resi accessibili nel loro significato e possa essere esercitata dal datore di lavoro un'attività valutativa e decisionale.
Seguendo tale ragionamento, gli strumenti tecnologici potrebbero essere considerati quali meri "strumenti di lavoro" fintanto che i dati acquisiti rimangano oscuri al datore di lavoro, ossia, prima dell'attività di elaborazione e correlazione.
In questa prospettiva, l'acquisizione di un dato privo di significato rimarrebbe al di fuori della sfera di controllo datoriale.
Permarrebbero, in ogni caso, le tutele inerenti alla *privacy* del lavoratore ove anche ai dati "non autoevidenti" venga riconosciuta la qualifica di dato personale.

606 Zappalà L., *Appunti su linguaggio, complessità e comprensibilità del lavoro 4.0: verso una nuova procedimentalizzazione dei poteri datoriali*, in *WP CSDLE "Massimo D'Antona".it*, n. 462, 2022, p. 8.

Uno strumento di lavoro diverrebbe, pertanto, di controllo solo nel momento in cui i dati "monitorati" venissero resi accessibili nel loro significato.
La distinzione tra "monitoraggio" e "controllo" trova riscontro anche nella cosiddetta "Scienza dei dati"[607] e nelle potenzialità delle nuove tecnologie informatiche che la rendono possibile.
L'accesso a dati non strutturati e la loro successiva integrazione, al fine di trarne valore, porta allo sviluppo di un modello analitico e organizzativo degli stessi finalizzato a comprenderne il significato.
La Scienza dei dati si sviluppa, infatti, secondo uno schema progressivo "a cascata" che viene di seguito riportato.



Modello di *pipeline*/cascata della scienza dei dati indicata quale Figura 9 nel contributo della prof.ssa Sonia Bergamaschi "*Il ruolo dei Dati nella trasformazione della società*", in Lavoro Diritti Europa, n. 3, 2022.

I primi quattro *task* (ovvero attività) del processo sono destinati a preparare i dati che verranno impiegati nella successiva elaborazione e sono "*un requisito indispensabile per ogni progetto che abbia l'obiettivo di trarre valore dai dati*"[608].
Tale fase, definita di *Data Integration*, risulta propedeutica e indispensabile al successivo passaggio di *Data Analysis*.
Il primo livello di intervento[609] che comporta, quindi, la raccolta di dati grezzi - ancora "non autoevidenti" - viene a identificarsi con un'attività di mero "monitoraggio", mancando un'organizzazione analitica che attribuisca significato ai dati.
La successiva fase di *Data Analysis* si identificherebbe, invece, con un effettivo "controllo".

La possibilità di distinguere, da un punto di vista informatico, tali fasi consente di programmare l'inserimento di interventi tecnici che prefigurino misure di sicurezza adeguate poste a separare i due processi (di *Data Integration* e *Data Analysis)* e a bloccare, così, un automatico passaggio da uno stadio di "monitoraggio" a uno di "controllo".

---

[607] In merito si rinvia al lavoro della professoressa Sonia Bergamaschi, Bergamaschi S., *Il ruolo dei Dati nella trasformazione della società*, in *Lavoro Diritti Europa*, n. 3, 2022.
[608] Bergamaschi S., *Il ruolo dei Dati nella trasformazione della società*, in *Lavoro Diritti Europa*, n. 3, 2022, p. 10.
[609] A parere dell'autrice, il processo di "*data cleaning*" dovrebbe, invece, risultare escluso dal "monitoraggio" ove comporti una selezione basata su una (anche parziale) comprensione dei dati raccolti.

Le misure di sicurezza dipendono, inevitabilmente, dal contesto specifico, ma tra gli strumenti a cui è possibile fare ricorso vi è, per esempio, la crittografia dei dati grezzi.
Crittografare i dati può impedirne l'analisi, in quanto i dati risultano accessibili solo se si è in possesso delle chiavi di decrittazione.
Un'ulteriore misura di sicurezza potrebbe essere l'adozione di sistemi di autenticazione robusti, come ad esempio l'autenticazione a più fattori (*Multi Factor Authentication*, MFA), posti ad autorizzare il passaggio dalla fase di *Data Integration* a quella di *Data Analysis* (ossia di controllo).
Tali strumenti consentono di aggiungere un livello di sicurezza supplementare, richiedendo plurime verifiche sull'identità prima di concedere l'accesso ad un sistema, ad un'applicazione o a un database di dati.
Chiaramente questa tutela vale soprattutto qualora vengano utilizzati per l'analisi servizi *cloud* o di terze parti, per il cui intervento è sempre consigliabile accertarsi che possano offrire certificati *standard* di sicurezza.
È, inoltre, possibile ipotizzare l'impiego di *file* di *log* mediante i quali monitorare le attività compiute sui dati "non autoevidenti". La funzione dei *file* di *log* è, infatti, assimilabile a quella di "registri" che tengono traccia delle operazioni compiute. Risultano, quindi, particolarmente utili per un'osservazione delle attività svolte nel corso del tempo sui dati grezzi e per la conseguente gestione delle prestazioni dei sistemi di analisi.
Per un'efficace attuazione delle misure di sicurezza qui proposte a delimitare il passaggio da una fase di "monitoraggio" a una di "controllo", rimane centrale l'intervento umano dato dall' "esperto di dominio", ovvero di colui che conosce il dominio applicativo e, dunque, le finalità che si intendono ottenere dall'analisi compiuta.
La precisa conoscenza dell'area di interesse in cui un determinato algoritmo o sistema di IA deve operare per la risoluzione di problemi specifici, determina il conseguente sviluppo del *software* secondo il modello più idoneo per analizzare e interpretare i dati.
La funzione dell'esperto di dominio sarà, dunque, non solo quella di pianificare come deve avvenire l'analisi per raggiungere un determinato obbiettivo (per esempio, analizzare la *performance* dei lavoratori), ma anche quella di pianificare l'inserimento delle misure di sicurezza più adeguate a inibire l'accessibilità ai dati "non autoevidenti" da parte dei sistemi algoritmici o di IA.

L'interpretazione fornita, basata sulle funzionalità di "monitoraggio" o "controllo" dello strumento, richiederebbe un aggiornamento[610] del dettato dell'art. 4 SL il quale riconosce l'esercizio del potere datoriale di controllo nel momento stesso in cui un dato viene acquisito, senza tenere in considerazione l'effettiva visibilità e comprensibilità dello stesso.
Ricostruzione che incide sull'intervento della tutela collettiva, abilitata ad acquisire informazioni afferenti alla sola installazione degli strumenti di controllo, rimettendo all'intervento individuale la protezione dell'utilizzabilità dei dati.

Infine, un'ultima ponderazione interessa la natura del nuovo potere "di controllo direttivo" e la considerazione dell'inevitabile osservabilità dei lavoratori in contesti digitali per fini diversi da quelli disciplinari.

[610] In merito alla necessità di un aggiornamento del dettato dell'art. 4 SL, con particolare riguardo ad un maggior coinvolgimento dei rappresentanti dei lavoratori, si rinvia a Corti M., *Potere di controllo e nuove tecnologie. Il ruolo dei partner sociali,* in *Labour & Law Issues (LLI),* vol. 9, n.1, 2023, pp. I 59 ss.; Ingrao A., *Controllo a distanza e privacy del lavoratore alla luce dei principi di finalità e proporzionalità della sorveglianza*, in *Labour & Law Issues (LLI),* vol. 9, n. 1, 2023, pp. I 102 ss.

Parlare, infatti, di un incremento di osservabilità dei lavoratori porta sicuramente a valutare i risvolti (e i rischi) che ineriscono al potere di controllo datoriale. Tuttavia, non può essere tralasciata la contingenza che "l'osservabilità" divenga per il datore di lavoro digitale inevitabile, anche quando il fine non sia connesso a quello tradizionalmente associato al potere di controllo.
Da qui la definizione di un "potere di controllo direttivo", proprio con l'intento di sottolineare la duplicità del monitoraggio compiuto: quello per "finalità classiche" di vigilanza disciplinare e quello realizzato per scopi ulteriori, come la gestione e l'organizzazione del lavoro.
Aspetti che, come si è avuto modo di approfondire nella ricerca, appaiono trascurati dalle norme cogenti. L'art. 4 SL, come riscritto nel 2015, risulta infatti legato a una concezione di controllo come preordinata all'esercizio del (solo) potere disciplinare, senza prendere in considerazione le ulteriori finalità che il monitoraggio può soddisfare.
Il datore di lavoro digitale si trova, dunque, in una situazione di *impasse* da cui fatica ad uscire: poter osservare i propri lavoratori nel contesto virtuale lo vincola a restrizioni che ne limitano l'azione.
Vincoli certamente condivisibili, in quanto posti a tutela dei prestatori, ma che conducono a un ineludibile cambio organizzativo. L'interazione datore di lavoro-prestatori diviene più complessa e soggetta a divieti prima sconosciuti.
Mentre, per esempio, in un contesto analogico il datore di lavoro poteva girare per gli uffici e condividere un caffè con i propri dipendenti, senza che ciò venisse qualificato necessariamente come "un esercizio di controllo", in un contesto digitale il "giro per gli uffici" e la "pausa caffè condivisa" vengono bollati come verifica delle presenze e dei tempi di lavoro.
La definizione di un "potere di controllo direttivo" e la necessità di esercitare un'osservazione dei lavoratori per scopi diversi da quelli sanzionatori, collima con l'esigenza di distinguere non solo il "monitoraggio" dal "controllo", ma anche di sottolineare la differenza tra osservazione compiuta per fini disciplinari o per altri scopi distinti, come quelli organizzativi.
Monitorare per "esigenze organizzative" non deve, quindi, più avere solo un'accezione di verifica dell'efficienza delle prestazioni dei lavoratori.
Le potenzialità di analisi e di osservazione introdotte dalla tecnologia possono, infatti, promuovere il benessere sul posto di lavoro e supportare lo sviluppo personale e professionale dei lavoratori.
Un tale orientamento potrebbe portare ad un'evoluzione delle tecniche di analisi secondo un approccio maggiormente orientato ai lavoratori, portando allo sviluppo di tecniche di *Data Driven* non più definibili come "*People Analytics"* bensì quali "*Analytics for People*".
La tecnologia potrebbe supportare la previsione predisponendo, per esempio, degli *allert* che segnalino l'acquisizione di dati personali e/o particolari dei lavoratori a seguito dell'elaborazione e ponendo in evidenza le finalità per cui l'analisi è stata programmata.
Gli stessi processi automatizzati potrebbero, inoltre, provvedere ad un immediato "oscuramento" delle informazioni sensibili acquisite a seguito dell'elaborazione, adottando tecniche di anonimizzazione, nonché informare tempestivamente gli interessati (o i loro rappresentanti) sulla natura dei dati acquisiti.
Ciò al fine di favorire una valutazione sulla necessità, o meno, di condividere tali informazioni con il datore di lavoro in riferimento alle esigenze di osservazione dichiarate.

Nonostante la distinzione tra "monitoraggio" e "controllo", ciò che traspare dal quadro delineato è una rinnovata manifestazione del potere datoriale.

Nel confrontarsi con le nuove realtà del lavoro digitale, la domanda "*quis custodiet ipsos custodes?*" trova una risposta di accomodamento in ragione della fluidità che caratterizza il modo di manifestarsi del potere di controllo tecnologico.

Al pari della scienza che non cerca conclusioni definitive, in quanto è un processo continuo di scoperta e apprendimento, anche il diritto non deve cercare soluzioni categoriche alle esigenze che possono derivare dall'impiego di sistemi algoritmici o di IA negli ambienti di lavoro.
Consapevole di ciò, la tutela dei lavoratori non potrà che individuare nuove risposte in riferimento alle necessità che la tecnologia solleverà, salvaguardando, però, il principio personalista che ha salde radici costituzionali e che si sostanzia nei diritti inviolabili dell'uomo[611].
Il principio funge da criterio orientativo dell'intera Carta repubblicana dato che il "*fine ultimo dell'organizzazione sociale*" è "*lo sviluppo di ogni singola persona umana*"[612], ma può essere ricavato anche da alcuni articoli in cui trova espressione.
L'articolo 2 della Costituzione italiana afferma, infatti, che la "*Repubblica riconosce e garantisce i diritti inviolabili dell'uomo*", assicurando in tal modo la protezione della persona umana da parte dell'ordinamento non solo sotto un profilo conservativo, ma tutelando anche lo sviluppo della stessa.
La tutela della persona e dei propri diritti - come la libertà e l'integrità fisica – trovano espressione anche in altre norme della Carta costituzionale che ne articolano le tutele, facendo riferimento al diritto di uguaglianza (art. 3 Cost.), alla libertà individuale (art. 13 Cost.) e al diritto alla salute (art. 32 Cost.).
Principio, quello personalista, ben noto a chi ha predisposto cinquant'anni fa lo Statuto dei Lavoratori e (ri)confermato quale criterio orientatore delle norme europee di prossima formulazione, quali la proposta di Regolamento sull'Intelligenza Artificiale o la proposta di Direttiva sulle piattaforme digitali.

La rilevanza posta al singolo e il conseguente approccio antropocentrico sottolinea il ruolo centrale che deve essere riservato all'uomo sul governo delle tecnologie (il cosiddetto *human on command*) e si riflette nelle nuove norme volte a garantire una sorveglianza umana sul funzionamento dei sistemi algoritmici e di IA.
L'autodeterminazione dei lavoratori e l'effettivo controllo delle decisioni che li coinvolgono sembra potersi realizzare pienamente attraverso un regime di "*governance* collaborativa"[613] ove la tutela non si realizza mediante norme di dettaglio, ma nello sviluppo di soluzioni personalizzate studiate per rispondere alle peculiarità che la tecnologia pone nei distinti contesti di lavoro.
Indirizzo offerto non solo dalle norme *de jure condito* del GDPR in materia di protezione dei dati personali, ma anche da quelle *de jure condendo* della proposta di Regolamento sull'IA e dalla proposta di Direttiva sul lavoro mediante piattaforma.
Per fare ciò, l'effettiva comprensione non solo degli strumenti, ma anche degli *input* (ossia i dati) si pone quel presupposto necessario ad ogni successivo intervento.

L'effettivo controllo umano sulla tecnologia trova, così, nella tutela della trasparenza un naturale sviluppo: limitare l'opacità delle elaborazioni previene l'ignoranza sul loro operato da cui deriva l'incontrollabilità del potere computazionale.

---

611 La definizione di inviolabilità dei diritti fondamentali legati alla persona ha implicato che a questi venissero attribuite qualifiche ulteriori quali le inabilità, le imprescrittibilità e l'indisponibilità. In riferimento all'art. 2 della Costituzione la dottrina discute genericamente di "diritti indisponibili". Cfr. Crisafulli V., Paladin L., *Commentario breve alla Costituzione,* Cedam, Padova, 1990, p. 11.
612 Corte costituzionale, sentenza n. 167 del 1999, punto 6 ultima parte.
613 Di "*collaborative governance*" fa riferimento Marta Otto in *A step towards digital self-& co-determination in the context of algorithmic management systems*, in *Italian Labour Law e-Journal*, n. 1, vol. 15, 2022, p. 62.

L'interrogativo su chi "controllerà i vigilanti"[614] rimane, dunque, un quesito attuale ove la manifestazione del nuovo "potere direttivo di controllo" schermata dietro un'apparente neutralità dei dati acquisiti, considerata anche la fluidità con cui si manifesta il controllo datoriale, necessita di altrettanta flessibilità nelle tutele.

Potere che, come si è avuto modo di illustrare, appare incontrastato ove non si offrano adeguati bilanciamenti al suo esercizio che consentano di rispettare i principi di dignità e proporzionalità mentre si osservano le tracce digitali lasciate dai lavoratori in contesti tecnologici.

Le tutele per essere valide devono sapersi collocare nel contesto in cui si vive, offrendo la possibilità di rispondere in modo adeguato alle sfide delle nuove tecnologie abilitanti.

Le inedite dinamiche dei rapporti di lavoro possono, però, trovare risposte adeguate ove lo sguardo venga volto ai principi fondamentali, verso cui il giuslavorista deve orientare la propria riflessione per comprendere e rispondere alle moderne esigenze dei prestatori digitali.

Riflessione condivisa anche dal Parlamento italiano che nel parere reso all'Unione europea sulla proposta di Regolamento sull'IA sottolinea come il coordinamento tra le diverse discipline, *de jure condito* e *de jure condendo*, deve evitare "*disallineamenti in grado di compromettere il raggiungimento dei rispettivi obiettivi, con particolare riguardo alla tutela dei diritti fondamentali*"[615].

[614] Il quesito "*quis custodiet ipsos custodes*" si legge nelle "Satire" di Giovanale Satire VI, verso 347). Giovenale utilizzò questa espressione per esprimere preoccupazioni sulla corruzione e l'abuso di potere all'interno della società romana. Nella sua satira, l'autore rifletteva sulle difficoltà di mantenere l'ordine e la giustizia quando gli incaricati di applicare le leggi potrebbero essere corrotti o abusare del loro potere.

[615] Pagina 4 lettera e) del parere del Parlamento italiano del 19 aprile 2022, documento 2021/0106(COD) visionabile integralmente al *link:* https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CONSIL:ST_8364_2022_INIT&from=IT

Bibliografia

Premessa e Capitolo 1

Adams-Prassl J., *What if Your Boss Was an Algorithm? Economic Incentives, Legal Challenges, and the Rise of Artificial Intelligence at Work*, in *Comparative Labor Law & Policy Journal 123*, vol. 41, n. 1, 2019, pp. 1 ss.

Aloisi A., *Regulating Algorithmic Management at Work in the European Union: Data Protection, Non-Discrimination and Collective Rights*, 2022, pp. 1 ss.

Aloisi A., De Stefano V., *Il tuo capo è un algoritmo. Contro il lavoro disumano,* Laterza, Bari, 2020.

Angeletti L., *Dignità e libertà della persona che lavora tra luoghi fisici e spazi immateriali*, in Mingione E., Scarpelli F., Giasanti L. (a cura di), *Lo Statuto dei lavoratori alla prova dell'oggi: Una rilettura critica da parte degli studiosi di nuova generazione,* Feltrinelli, Milano, 2022.

Angrave D., Charlwood A., Kirkpatrick I., Lawrence M., Stuart M., *HR and Analytics: Why HR Is Set to Fail the Big Data Challenge,* in *Human Resource Management Journal*, vol. 26, no. 1, 2016.

Ara K., Akitomi T., Sato N., Tsuji, S., Hayakawa M., Wakisaka Y. et All, *Healthcare of an organization: Using wearable sensors and feedback system for energizing workers,* in *Proceedings of the 16th Asia and South Pacific Design Automation Conference ASPDAC,* IEEE, January 2011.

Banno R., Takeuchi S. et all, *Designing overlay networks for handling exhaust data in a distributed topic-based pub/sub architecture,* in *Journal of Information Processing*, vol. 23, n. 2, pp. 105 ss.

Benadusi L., Molina S., *Le competenze. Una mappa per orientarsi*, Fondazione Agnelli, Il Mulino, Bologna, 2018.

Biagi M., Treu T., *Lavoro e Information Technology: riflessioni sul caso italiano*, in *Diritto della Relazioni Industriali (DRI*), n. 1, 2002, pp. 5 ss.

Brollo M., *Disciplina delle mansioni (art. 3)* in Carinci F. (a cura di), *Commento al D.Lgs. 15 giugno 2015, n. 81: le tipologie contrattuali e lo jus variandi,* ADAPT University Press, ADAPT Labour Studies e-Book series, 2015, n. 48, pp. 29 ss.

Brollo M., *Tecnologie digitali e nuove professionalità*, in *Diritto della Relazioni Industriali (DRI*), n. 2, 2019.

Cappellazzo N., *Algoritmi, automazione e meccanismi di intelligenza artificiale: la classificazione proposta dal Consiglio di Stato*, in *Federelismi.it* del 23 marzo 2022, pp. 1 ss.

Caruso B., *Strategie di flessibilità funzionale e di tutela dolo il Jobs Act: fordismo, post fordismo e industria 4.0*, in *Giornale di Diritto del Lavoro e di Relazioni Industriali (DLRI),* n. 1, 2018.

Chan C. F., Eric W. M., *An abnormal sound detection and classification system for surveillance applications*, in *Signal Processing Conference, 2010 18th European,* IEEE, August 2010.

Cipriani A., Gramolati A., Mari A. (a cura di), *La Quarta Rivoluzione industriale e le trasformazioni delle attività lavorative*, Firenze University Press, 2018, disponibile *online.*

Collins L., Fineman, D. R., Tshuchica, A., *People analytics: Recalculating the route», Deloitte Insights*, 2017, Disponibile *online*: https://www2.deloitte.com/insights/us/en/focus/human-capital-trends/2017/people- analytics-in-hr.html.

Comandè G., *Intelligenza artificiale e responsabilità tra* liability *e* accountability. *Il carattere trasformativo dell'IA e il problema della responsabilità*, in *Analisi giuridica dell'economia*, n. 1, 2019, pp. 169 ss.

Curzi Y., Pistoresi B., Fabbri T, *Understanding the stressful implications of remote e-working: Evidence from Europe*, Working paper, Demb Working Paper Series, Dipartimento di Economia Marco Biagi - Università di Modena e Reggio Emilia, 2020.

Dagnino E., *Dalla fisica all'algoritmo: una prospettiva di analisi giuslavoristica,* ADAPT University Press, 2019.

Dagnino E., *People Analytics: lavoro e tutele al tempo del management tramite big data,* in *Labor & Law Issue (LLI)*, vol. 3, n. 1, 2017, pp. I 1- I 31.

De Padova C., *La nuova frontiera dell'IT (Information Technology*), in *Rivista degli infortuni e delle malattie professionali,* 2013, n. 1-2, pp. 247 ss.
Del Giglio I., *Valutazione della performance mediante tecniche di People Analytics. Privacy in employment, controllo o innovazione?*, in *Journal of Ethics and Legal Technologies (JELT*), n. 11, 2021, pp. 103 ss.
Del Punta R., *Un diritto per il lavoro 4*.0, in Cipriani A., Gramolati A., Mari G (a cura di), *Il lavoro 4.0. La IV rivoluzione industriale e le trasformazioni delle attività lavorativ*e, FUP, Firenze, 2017.
Dessì O. *Il Controllo a distanza sui lavoratori. Il nuovo art. 4 Stat. lav*., Edizioni Scientifiche Italiane, Napoli, 2017.
Di Meo R., *Tecnologie e poteri datoriali: commento a margine del c.d. braccialetto Amazon*, in *Labour & Law Issues (LLI)*, vol. 4, n. 1, 2018, pp. R 1 – 19.
Diego-Mas J. A., Alcaide-Marzal, J., *Using KinectTM sensor in observational methods for assessing postures at work*, in *Applied Ergonomics*, vol. 45, n. 4, 2014, pp. 976 ss.
Donini A., *Tecniche avanzate di analisi dei dati e protezione dei lavorator*i, in *Diritto delle Relazioni Industriali*, n. 1, 2018, pp. 222 ss.
Fabbri T., Scapolan A. C., *Digitalization and Hr Analytics: A big game for an HR manager*, in Cantoni F., Mangia G. (a cura di), *Human Resource Management and Digitalization*, Giappichelli Routledge, 2018.
Faioli M., *Data Analytics, robot intelligenti e regolazione del lavoro*, in Focus lavoro, persona, tecnologia del 23 marzo 2022 su *Federalismi.it*, pp. 149 ss.
Gaudio G., *L'algorithmic management e il problema dell'opacità nel diritto oggi vigente e nella Proposta della Direttiva sul miglioramento delle condizioni dei lavoratori tramite piattaforma*, in *Lavoro Diritti Europa*, n. 1, 2022, p. 1 ss.
Gragnoli E., *Gli strumenti di controllo e mezzi di produzione*, in *Variazioni su Temi di Diritto del Lavoro*, n. 4, 2016, pp. 651 ss.
Greco L., *Tempo per lo spazio: riflessioni sui "luoghi" di lavoro*, in *Labour & Law Issues (LLI)*, vol. 9., n. 1, 2023, pp. 1 ss.
Harrag F., *Text mining approach for knowledge extraction in Sahîh Al-Bukhari*, in *Computers in Human Behavior*, vol.30, 2014, pp. 558 ss.
Ingrao A, Donini A., *Algoritmi e lavoro*, in *Labour Law Community* del 25 maggio 2022, consultabile *online* https://www.labourlawcommunity.org/ricerca/algoritmi-e-lavoro/.
Ingrao A, *Il controllo a distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata*, Cacucci Editore, Bari, 2018.
Ingrao A., *Data-Driven management e strategie collettive di coinvolgimento dei lavoratori per la tutela della privacy* in *Labour & Law Issues (LLI*), vol.5, n. 2, 2019, pp. 127–143.
Kim P.T., *Data-Driven Discrimination at Work*, in *William and Mary Law Review*, n. 58, 2017, pp. 587 ss.
Koriat, N., & Gelbard, R., *Knowledge sharing motivation among IT personnel: Integrated model and implications of employment contracts,* in *International Journal of Information Management*, vol. *34*, n. 5, 2014, pp. 577 ss.
Koriat, N., & Gelbard, R., *Knowledge sharing analytics: The case of IT workers*, in *Journal of Computer Information Systems*, vol. 59, n. 4, 2017, pp. 1–11.
Loi P.,*Il rischio proporzionato nella proposta di regolamento sull'IA e i suoi effetti nel rapporto di lavoro*, in *Federalismi.it,* n.4, 2023, pp. 239 ss.
Lombardi M., Macchi M., *Il lavoro tra intelligenza artificiale e intelligenza umana*, in Cipriani A., Gramolati A., Mari A. (a cura di), *La Quarta Rivoluzione industriale e le trasformazioni delle attività lavorative*, Firenze University Press, 2018.
Lombardi M., Macchi M., *Il lavoro tra intelligenza umana e intelligenza artificiale*, in Cipriani A., Gramolati A., Mari G (a cura di), Il lavoro 4.0. *La IV rivoluzione industriale e le trasformazioni delle attività lavorative*, FUP, Firenze, 2017.

Mantelero A., *Big Data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo,* in *Diritto dell'Informazione e dell'Informatica*, n. 1, 2012, pp. 135 ss.
Mantelero A., *Rilevanza e tutela della dimensione collettiva della protezione dei dati personali*, in *CI/Europa*, n. 1, 2015, pp. 137 ss.
Martini D., *Industria 4.0: una prima riflessione critica,* in *L'industria*, n. 3, 2016, pp. 383 ss.
Mateescu A., Nguyen A., *Algorithmic management in the workplace,* in *Data & Society Research Institute*, February 2019, pp. 1 ss.
Marazza M., *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore*), in *WP CSDLE "Massimo D'Antona".it*, n. 300, 2016, pp. 291 ss.
Mittelstandt B.D., Allo P., Taddeo M. et al., *The ethics of algorithms: Mapping the debate*, in *Big data & Society*, vol. 3, n. 2, 2016.
Oleary D., Storey V. C., *Discovering and Transforming Exhaust Data to Realize Managerial Value*, in Communications of the Association for Information Systems, vol. 47, paper 15.
Peruzzi M., *Il diritto antidiscriminatorio al test di intelligenza artificiale*, in *Labour & Law Issues (LLI)*, vol. 7, n. 1, 2021, pp. I 48 – I 76.
Piccinini I., Isceri M., *IA e datori di lavoro: verso una e-leadership?,* in *Lavoro Diritti Europa*, n. 2, 2021, pp. 1 ss.
Pisani C., *Rapporto di lavoro e nuove tecnologie: le mansioni*, in *Giornale del Diritto del Lavoro e delle Relazioni Industriali (DLRI),* n. 2, 1988, pp. 293 ss.
Politecnico di Milano, *White Paper*. Osservatorio *HR Innovation Practice* (2016). "*HR Analytics & Big Data Driven Innovation: cosa significa e come impostare una roadmap di innovazione*". In collaboration with Cornerstone.
Popma J., *The Janus face of the 'New Way of Work' Rise risk and regulation of nomadic work*, in *ETUI Working Paper*, n. 7, 2013.
Portinale L., *Intelligenza Artificiale: storia, progressi e sviluppi tra speranze e timori*, in *Media Laws*, n. 3, 2021, pp. 13 ss.
Preece S. J., Goulermas J. Y., Kenney L. P. J., Howard D., Meijer K., Crompton R., *Activity identification using body-mounted sensors—A review of classification techniques,* in *Physiological Measurement*, vol. 30, n. 4, 2009, pp. R 1 ss.
Punnoose R., Ajit P., *Prediction of employee turnover in organizations using machine learning algorithms*, in *International Journal of Advanced Research in Artificial Intelligence (IJARAI)*, vol. 5, n. 9, 2016.
Robinson S. D., Sinar E., Winter J, *Social media as a tool for research: A turnover application using LinkedIn*, in *TIP: The Industrial-Organizational Psychologist*, vol 52, n.1, 2014.
Rosário J. L., Diógenes M. S. B., Mattei R., Leite J. R., *Angry posture*, in *Journal of Bodywork and Movement Therapies*, n. 20(3), 2016.
Rosário J. L., Diógenes M. S. B., Mattei R., Leite J. R., *Differences and similarities in postural alterations caused by sadness and depression*, in *Journal of Bodywork and Movement Therapies*, vol. 18, n. 4, 2014.
Rota A*., Rapporto di lavoro e big data analytics: profili critici e risposte possibili*, in *Labour & Law Issues (LLI)*, vol.3, n.1, 2017, I 32 – 52.
Rota A., *Sull'Accordo Quadro europeo in tema di digitalizzazione del lavoro,* in *Labour & Law Issues (LLI),* vol. 6, n. 2, 2020, C 23 – C 48.
Royal Society (UK), *Machine learning: the power and promise of computers that learn by example* (April 2017).
Ruffolo U., *Intelligenza artificiale, machine learning e responsabilità da algoritmo*, in *Giurisprudenza Italiana*, n. 7, 2019.
Sanguinetti G., *Machine Learning: accuratezza, interpretabilità e incertezza*, in *Ithaca: Viaggio nella Scienza*, n. 16, 2020, pp. 71 ss.

Santucci R., *La quarta rivoluzione industriale e il controllo a distanza dei lavoratori*, in *Il Lavoro nella giurisprudenza,* n. 1, 2021, pp. 19 ss.
Sartor G., *L'informatica giuridica e le tecnologie dell'informazione. Corso d'informatica giuridica*, Terza edizione Giappichelli, Torino, 2016.
Seghezzi F., *La nuova grande trasformazione. Lavoro e persona nella quarta rivoluzione industriale*, ADAPT University Press, 2017.
Seghezzi F., *Le grandi trasformazioni del lavoro, un tentativo di periodizzazione. Appunti di ricerca,* Working Paper ADAPT University Press, 2015.
Senatori I., *The European Framework Agreement on Digitalisation: a Whiter Shade of Pale,* in *Italian Labour Law e Journal,* vol. 13, n. 2, 2021, pp. 159 ss.
Sigismondi I., *Telematica*, voce in *Diritto Costituzionale*, Treccani consultabile sul sito https://www.treccani.it/enciclopedia/telematica-dir-cost_%28Diritto-on-line%29/.
Spincer A., Alvesson M., Karreman D., *Resisting resistance. Critical performativity. The unfinished business of critical management studies*, in *Human Relations*, vol. 62, n. 4, 2009.
Stefano N., *La disciplina del Data Mining alla luce della proposta di regolamento comunitario in materia di trattamento di dati personali: criticità, limiti e prospettive de jure condendo*, in *FiloDiritto*, 20 aprile 2015, disponibile al sito: https://is.gd/P9YLmW.
Stizia A., *Personal computer e controlli "tecnologici" del datore di lavoro nella giurisprudenza*, in *Argomenti di Diritto del Lavoro (ADL),* n. 3, 2017, pp. 804 ss.
Stizia A., Lopez B., *Le più avanzate modalità di controllo sul lavoratore: machine learning e social media*, in Pisani C., Proia G., Topo A. (a cura di) *Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro*, Giuffrè Editore, Milano, 2022.
Subhashini R., Niveditha, P. R., *Analyzing and detecting employee's emotion for amelioration of organizations,* in *Procedia Computer Science*, n. *48*, 2015, pp. 137 ss.
Tebano L, *Fabbrica 4.0 e potere di "controllo direttivo"*, in Rusciano M., Gaeta L., Zoppoli L. (a cura di), *Mezzo secolo dallo statuto dei lavoratori*, in *Quaderni della Rivista Diritti Lavori Mercanti, n. 8, 2020, pp.,* 443 ss.
Tebano L., *Lavoro, potere direttivo e trasformazioni organizzative*, Editoriale Scientifica, Napoli, 2020.
Tebano L*., La digitalizzazione del lavoro tra intelligenza artificiale e gestione algoritmica*, in *IANUS*, n. 24, 2021, pp. 43 ss.
Tebano L., *Poteri datoriali e dati biometrici nel contesto dell'AI Act*, in *Federalismi.it*, n. 25, 2023, pp. 198 ss.
Tufo M., *Lo Statuto dei lavoratori alla prova della Quarta Rivoluzione Industriale*, in Mingione E., Scarpelli F., Giasanti L. (a cura di), *Lo Statuto dei lavoratori alla prova dell'oggi: Una rilettura critica da parte degli studiosi di nuova generazione,* Feltrinelli, Milano, 2022.
Tietz Cazeri G., De Santa-Eulalia L. A., Pavan Serafim M., Anholon R., *Training for Industry 4.0: a systematic literature review and directions for future research,* in *Brazilian Journal of Operations & Production Management*, vol. 19, n. 3, 2022, pp. 1 ss.
Tiraboschi M., Seghezzi F., *Il Piano nazionale Industria 4.0: una lettura lavoristica*, in *Labour & Law Issues (LLI),* vol. 2, n. 2, 2016, pp. I 1 -41.
Treu T*., La digitalizzazione del lavoro: proposte europee e piste di ricerca,* in *Federalismi.it*, n. 9, 2022.
Tullini P., *Il controllo a distanza attraverso gli strumenti per rendere la prestazione lavorativa. Tecnologie di controllo e tecnologie di lavoro: una distinzione possibile*, in Tullini P. (a cura di) *Controlli a distanza e tutela dei dati personali*, Giappichelli Editore, Torino, 2017.
Valenduc G., Vendramin P., *Work in the digital economy: sorting the old from the new*, ETUI Working Paper, n. 3, 2016, pp. 1 ss.
Van Zoonen W., Verhoeven J. W. M., Vliegenthart R., *How employees use Twitter to talk about work: A typology of work-related tweets,* in *Computers in Human Behavior*, n. 55, 2016, pp. 329 ss.

Wood A., *Algorithmic management Consequences for Work Organisation and Working Conditions*, in *JRC Working Papers Series on Labour, Education and Technology*, n. 7, 2021, pp. 1 ss.
Zanetti P., *Impresa, lavoro e innovazione tecnologica*, Giuffrè Editore, Milano, 1985.
Zeno-Zencovich V., Giannone Codiglione G., *Ten legal perspective on the "big data revolution*", in *Concorrenza e Mercato*, vol. 23, 2016, pp. 29 ss.
Zuddas P., *Intelligenza Artificiale e discriminazioni,* in *Consulta OnLine*, 16 marzo 2020, pp. 1 ss

Capitolo 2.1

Adams-Prassl J., *What if Your Boss Was an Algorithm? Economic Incentives, Legal Challenges, and the Rise of Artificial Intelligence at Work*, in *Comparative Labor Law & Policy Journal 123*, vol. 41, n. 1, 2019, pp. 1 ss.
Aimo M., *Privacy, libertà di espressione e rapporto di lavoro*, Jovene, Napoli, 2003.
Aloisi A., De Stefano V., *Il tuo capo è un algoritmo. Contro il lavoro disumano,* Laterza, Bari, 2020.
Alvino I, *L'art. 4 Stat. lav. alla prova di internet e della posta elettronica*, in *Diritto delle Relazioni Industriali (DRI),* n. 4, 2014, pp. 999 ss.
Alvino I., *I nuovi limiti al controllo a distanza dell'attività dei lavoratori nell'intersezione fra le regole dello Statuto dei lavoratori e quelle del Codice della privacy*, in *Labour & Law Issues (LLI)*, vol. 2, n. 1, 2016, pp. 1-45.
Arbore A., *La nuova disciplina dei controlli ex art. 4 St. lav.*, in Ghera E., Garofalo D. (a cura di), *Semplificazioni sanzioni, ispezioni nel Jobs Act 2,* Cacucci Editore, Bari, 2016.
Baletti E., *I poteri del datore di lavoro tra legge e contratto*, relazione tenuta in occasione delle Giornate di Studio Aidlass, Napoli, 16-17 giugno 2016, in www.aidlass.it.
Bandelloni G., *La rimozione del divieto di controllo a distanza: significato e conseguenze*, in *Rivista Giuridica del Lavoro (RGL)*, n. 1, 2018, pp. 85 ss.
Bellavista A., *I poteri dell'imprenditore e la privacy del lavoratore*, in *Il Diritto del Lavoro*, vol. 76, fasc. 3., 2002, pp. 183 ss.
Bellavista A., *Il controllo sui lavoratori*, Giappichelli, Torino, 1995.
Bellavista A., *Il nuovo art. 4 dello Statuto dei lavoratori,* in Zilio Grandi G., Biasi M. (a cura di), *Commentario breve alla riforma "Jobs Act",* WK Cedam, 2016.
Busacca A., *Sub art. 88*, in Riccio G. M., Scorza G., Bellisario E. (a cura di), *GDPR e normativa privacy. Commentario,* Wolters Kluwer, Milano, 2018.
Caricci M. T., *Il controllo a distanza dell'attività dei lavoratori dopo il "Jobs Act" (art. 23 D.Lgs. 151/2015): spunti per un dibattito,* in *Labour & Law Issues (LLI)*, vol. 2, n. 1, 2016, pp. I-XIV.
Carinci M. T., *Il controllo a distanza sull'adempimento della prestazione di lavoro*, in Tullini P. (a cura di) *Controlli a distanza e tutela dei dati personali del lavoratore*, Giappichelli Editore, Torino, 2017.
Casillo R., *La dignità nel rapporto di lavoro*, in *Rivista di Diritto Civile*, n. 5, 2008, pp. 593 ss.
Cataudella A., *Sub art. 4,* in Prosperetti U. (a cura di), *Commentario della Statuto dei Lavoratori,* Giuffrè Editore, Milano, 1975.
Cester C., Mattarolo M. G., *Diligenza e obbedienza del prestatore di lavoro. Art. 2104*, in Schlesinger P. (a cura di), *Il Codice Civile. Commentario*, Giuffrè Editore, Milano, 2007.
Crisafulli V., *Diritti di libertà e poteri dell'imprenditore*, in *Rivista Giuridica del Lavoro (RGL)*, n. 1, 1954, pp. 190 ss.
D'Antona M., *L'art. 4 dello Statuto dei Lavoratori ed elaborati elettronici*, in De Luca-Tamajo R., Imperiali-D'Afflitto R., Pisani. C., Romei R. (a cura di), *Nuove tecnologie e tutela della riservatezza del lavoratore*, Giuffrè Editore, Milano, 1988.
Dagnino E. *Tecnologie e controlli a distanza*, in *Diritto delle Relazioni Industriali (DRI)*, n. 4, 2015, pp. 988 ss.

De Luca Tamajo R., *Introduzione*, in Tullini P. (a cura di) *Tecnologie della comunicazione e riservatezza nel rapporto di lavoro*, in Galgano F. (diretto da), *Trattato di diritto commerciale e diritto pubblico dell'economia*, Cedam, Padova, vol. 1, 2010.
Del Punta R., *La nuova disciplina dei controlli a distanza sul lavoro (art. 23, d. lgs. n. 151/2015*), in *Rivista Italiana del Diritto del Lavoro (RIDL)*, vol. 1, 2016, pp. 77 ss.
Dessì O., *Il controllo a distanza sui lavoratori. Il nuovo art. 4 Stat. Lav.*, Edizioni Scientifiche Italiane, Napoli 2017.
Ficari L., *I controlli effettuati attraverso gli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa,* in Levi A. (a cura di), *Il nuovo art. 4 sui controlli a distanza. Lo statuto dei lavoratori dopo il Jobs Act,* Giuffrè Editore, 2016.
Frattini R., Maurelli R., *La nuova disciplina dei controlli a distanza nel dialogo fra art. 4 e codice privacy,* in *Lavoro e previdenza oggi*, 11-12/2020, pp. 714 ss.
Fregni A., Giugni G., *Lo Statuto dei Lavoratori. commentario alla legge 20 maggio 1970 n. 300,* Giuffrè Editore, Milano, 1971.
Gaudio G., *L'algorithmic management e il problema dell'opacità nel diritto oggi vigente e nella Proposta della Direttiva sul miglioramento delle condizioni dei lavoratori tramite piattaforma*, in *Lavoro Diritti Europa*, n. 1, 2022, pp. 1 ss.
Gragnoli E., *L'informazione nel rapporto di lavoro*, Giappichelli Editore, Torino, 1996.
Gragnoli E., *L'uso della posta elettronica sui luoghi di lavoro e la strategia elaborata dall'Autorità Garante,* in Tullini P. (a cura di) *Tecnologie della comunicazione e riservatezza nel rapporto di lavoro*, in Galgano F. (diretto da), *Trattato di diritto commerciale e diritto pubblico dell'economia*, Cedam, Padova, vol. 1, 2010.
Grandi M., Pera G., *Sub Art. 4*, in *Commentario alla Statuto dei lavoratori*, Cedam, Padova, 1972.
Grillo Pasquarelli F., *Gli strumenti di controllo a distanza dei lavoratori*, Relazione tenuta all'incontro di studio "Jobs Act *dopo 5 anni: un quadro aggiornato della giurisprudenza*", organizzato dalla SSM, Scandicci, 13 - 15 gennaio 2020.
Ichino P., *Diritto alla riservatezza e diritto al segreto nel rapporto di lavoro*, Giuffrè Editore, 1979, Milano.
Ichino P., *Introduzione*, in A. Sartori, *Il controllo tecnologico sui lavoratori*, Giappichelli Editore, Torino, 2020.
Ingrao A*, I controlli difensivi tra passato e presente: privacy del lavoratore e inutilizzabilità dei dati*, in *La nuova giurisprudenza civile commentata*, n. 4, 2019, pp. 649 ss.
Ingrao A., *Data-Driven management e strategie di coinvolgimento collettivo dei lavoratori per la tutela della privacy,* in *Labour & Law Issues (LLI)*, n. 2, 2019, pp. 127–143.
Ingrao A., *Il controllo a distanza sui lavoratori*, Cacucci Editore, Bari, 2018.
Ingrao A., *Il controllo difensivo sugli atti illeciti dei lavoratori da parte di agenzie investigative tra Statuto dei lavoratori, Testo Unico di Pubblica Sicurezza e normativa a protezione dei dati personali,* in *Labor,* n. 1, 2023, pp. 69 ss.
Ingrao A., *Il controllo disciplinare e la privacy del lavoratore dopo il Jobs Act,* in *Rivista Italiana di Diritto del Lavoro*, vol. 36, n. 1, 2017, pp. 46 ss.
Lanotte M., *La ridefinizione dei limiti al potere di controllo a distanza*, in A. Levi (a cura di), *Il nuovo art. 4 sui controlli a distanza. Lo Statuto dei Lavoratori dopo il Jobs Act*, Giuffrè Editore, Milano, 2016.
Levi A., *Il controllo informatico sull'attività del lavoratore,* Giappichelli Editore, Torino, 2013.
Levi A., *Il potere di controllo dell'imprenditore sull'uso degli strumenti di lavoro e le tecnologie informatiche,* in *Un diritto in evoluzione. Studi in onere di Yasui Suwa,* a cura di L. Montuschi, Giuffrè Editore, Milano 2007.
Levi A., *La ridefinizione dell'assetto regolativo dei controlli a distanza, quale tassello di una più complessiva riforma del diritto del lavoro*, in Levi A. (a cura di), *Il nuovo art. 4 sui controlli a distanza. Lo Statuto dei Lavoratori dopo il Jobs Act*, Giuffrè Editore, Milano, 2016.
Maio V., *La nuova disciplina dei controlli a distanza sull'attività dei lavoratori e la modernità post panottica,* in *Argomenti di Diritto del Lavoro (ADL)*, n. 6, 2015, pp. 1186 ss.

Marazza M., *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore), in Argomenti di Diritti del Lavoro (ADL),* vol. 21, n. 3, 2016, pp. 483 ss.
Marazza M., *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore)* in WP CSDLE "Massimo D'Antona".it – 300/2016, pp. 291 ss.
Maresca A., *Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 dello statuto dei lavoratori,* in *Rivista Italiana del Diritto del Lavoro (RIDL)*, vol. 1, 2016, pp. 513 ss.
Maresca A., *Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 St. lav.*, in Tullini P. (a cura di) *Controlli a distanza e tutele dei dati personali dei lavoratori,* Giappichelli Editore, Torino, 2017.
Maresca A., *Jobs Act, come conciliare potere di controllo e tutela della dignità e riservatezza del lavoratore,* in *Forum Tutto lavoro Ipsoa*, 2016.
Mateescu A., Nguyen A., *Algorithmic management in the workplace,* in *Data & Society Research Institute*, February 2019.
Pera G., *Sub art. 4*, in Assanti C., Pera G (a cura di) *Commento alla Statuto dei Lavoratori*, Cedam, Padova, 1972.
Perulli A., *Razionalità e proporzionalità nel diritto del lavoro*, *in Giornale di Diritto del Lavoro e di Relazioni Industriali*, vol. 1, 2005, pp. 1 ss.
Proia G., *Trattamento dei dati personali, rapporti di lavoro e "l'impatto" della nuova disciplina dei controlli a distanza,* in *Rivista Italiana di Diritto del Lavoro*, fasc. 4, 2016, pp. 547 ss.
Romagnoli U., *Sub Art. 4*, in Ghezzi G., Mancini G. F., Montuschi L., Romangnoli U. (a cura di) *Statuto dei diritti dei lavoratori*, Ed. Universitaria, Bologna, 1972.
Russo A., Tufo M., *I controlli preterintenzionali: la nozione*, in Levi A. (a cura di) *Il nuovo art. 4 sui controlli a distanza. Lo statuto dei Lavoratori dopo il Jobs Act*, Giuffrè Editore, Milano, 2016.
Russo M., *Quis custodiet ipsos custodes? I "nuovi" limiti all'esercizio del potere di controllo a distanza*, in *Labour & Law Issues (LLI),* vol. 2, n. 2, 2016, R 1-26.
Santoro Passarelli G., *Osservazioni in tema di art. 3 e 4 stat. lav*, in *Diritto del Lavoro*, vol. I, 1986, pp. 460 ss.
Santucci R., *La quarta rivoluzione industriale e il controllo a distanza dei lavoratori*, in *Il Lavoro nella giurisprudenza,* n. 1, 2021, pp. 19 ss.
Sartori A., *Il controllo tecnologico sui lavoratori. La nuova disciplina italiana tra vincoli sovranazionali e modelli comportamentali,* Giappichelli Editore, Torino, 2020.
Scagliarini S. (a cura di), *Il "nuovo" codice in materia di protezione dei dati personali,* Giappichelli Editore, Torino, 2019.
Smuraglia C., *Progresso tecnico e tutela della personalità del lavoratore*, in *Rivista Giuridica del Lavoro*, Vol. 1, 1960, pp. 312 ss.
Stizia A., *I controlli a distanza dopo il "Jobs Act" e la Raccomandazione R(2015)5 del Consiglio d'Europa*, in *Il Lavoro nella Giurisprudenza*, n. 7, 2015, pp. 671 ss.
Stizia A., *Il controllo (del datore di lavoro) sull'attività dei lavoratori: il nuovo art. 4 st. lav. e il consenso del lavoratore*, in *Labour & Law Issues (LLI),* vol. 2, n. 1, 2016, pp. 82 ss.
Stizia A., *Il decreto legislativo di attuazione del Regolamento Privacy (n. 101 del 2018): profili giuslavoristici,* in *Lavoro Diritti Europa*, vol. 1, n. 2, 2018.
Stizia A., *Personal computer e controlli "tecnologici", del datore di lavoro nella giurisprudenza*, in *Argomenti di Diritto del Lavoro (ADL),* n. 3, 2017, pp. 804 ss.
Tebano L., *Lavoro, potere direttivo e trasformazioni organizzative*, Editoriale Scientifica, Napoli, 2020.
Trojsi A., *Potere informatico del datore di lavoro e controllo sui lavoratori, cinquant'anni dopo*, in *Dirittifondamentali.it*, fasc. 2, 2020, pp. 1411.
Tullini P. (a cura di), *Controlli a distanza e tutela dei dati personali dei lavoratori*, Giappichelli Editore, Torino, 2017.

Tullini P., *Comunicazione elettronica, potere di controllo e tutela del lavoratore,* in *Rivista Italiana del Diritto del Lavoro*, vol. 1, 2009, pp. 323 ss
Tullini P., *Il controllo a distanza attraverso gli strumenti per rendere la prestazione lavorativa. Tecnologie di controllo e tecnologie di lavoro: una distinzione possibile?* in Tullini P. (a cura di, in), *Controlli a distanza e tutela dei dati personali del lavoratore*, Giappicheli Editore, Torino, 2017.
Vallauri M. L., *È davvero incontenibile la forza espansiva dell'art. 4 dello Statuto ei lavoratori*, in *Rivista Italiana di Diritto del Lavoro*, vol. 3, 2008, pp. 718 ss.
Zagrebelsky G., *Giustizia costituzionale*, Il Mulino, Bologna, 2012.
Zoli C., *Il controllo a distanza del datore di lavoro: l'art. 4, l. n. 300/1970 tra attualità ed esigenze di riforma*, in *Rivista Italiana di Diritto del Lavoro*, vol. 1, 2009, pp. 485 ss.
Zoli C., Il controllo a distanza dell'attività dei lavoratori e la nuova struttura dell'art. 4, legge n. 300/1970, in Variazione sui Temi di Diritto del Lavoro, n. 4, 2016, pp. 635 ss.
Zoli C., Villa E., *Gli strumenti di registrazione degli accessi e delle presenze*, in *Controlli a distanza e tutela dei dati personali del lavoratore*, in P. Tullini (a cura di), Giappichelli, Torino, 2017.

Capitolo 2.2.

Ales E., *Is performance appraisal compatible with the employment relationship? A conclusive plea in favour of an achievement-oriented approach to work organization*, in Addabbo T., Ales E., Curzi Y., Fabbri T., Rymkevich O., Senatori I. (eds.), *Performance Appraisal in Modern Employment Relations. An Interdisciplinary Approach*, Palgrave Macmillan, Cham, 2020.
Alvino I., *I nuovi limiti al controllo a distanza dell'attività dei lavoratori nell'intersezione fra le regole dello Statuto dei lavoratori e quelle del Codice della privacy*, in *Labour & Law Issues (LLI),* vol. 2, n. 1, 2016, pp. 1-45.
Bertolli F., Fabbri T., Mandreoli F., Martoglia R., Scapolan A. C., *Work datafication and digital work behavioranalysis as a source of social good,* Conference Paper 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC).
Bogdan R., Tatu A., Crisan-Vida M. M., Popa M., Stoicu-Tivadar L., *A practical experience on the Amazon Alexa integration in smart offices*, in *Sensors*, vol. 21, n. 734, 2021, pp. 1 ss.
Cairo L., *Il controllo a distanza dei lavoratori: precedenti nella giurisprudenza di ieri decisi con la norma di oggi*, in *Labour & Law Issues (LLI)*, vol. 2, n. 1, 2016, pp. 60-80.
Cataudella A., *Sub. art. 8*, Giuffrè Editore, Milano, 1975.
Cherry M. A., *People Analytics and invisible labor*, in *Saint Louis University Law Journal*, vol. 61, n. 1, 2016.
Curzi Y., Fabbri T. e Pistoresi B., *Performance appraisal criteria and innovative work behaviour: the mediati grole of employees' appraisal satisfaction*, in Addabbo T., Ales E., Curzi Y., Fabbri T., Rymkevich O., Senatori I. (eds.), *Performance Appraisal in Modern Employment Relations. An Interdisciplinary Approach*, Palgrave Macmillan, Cham, 2020.
Curzi Y., Fabbri T., Scapolan A. C., Boscolo S., *Performance appraisal and innovative behavior in digital era*, in *Frontiers in Psycology,* Vol. 10, July 2019.
D'Antona M., *L'art. 4 dello Statuto dei Lavoratori ed elaborati elettronici*, in De Luca Tamajo R., Imperiali D'Afflitto R., Pisani C., Romei R. (a cura di), *Nuove tecnologie e tutela della riservatezza del lavoratore*, Giuffrè Editore, Milano, 1988.
Dagnino E., *Dalla fisica all'algoritmo: una prospettiva di analisi giuslavoristica*, ADAPT University Press, 2019.
Dagnino E., *Il diritto alla disconnessione nella legge n. 81/2017 e nell'esperienza comparata*, in *Diritto della Relazioni Industriali (DRI),* n. 4, 2017, pp. 1024.
Dagnino E., *Le tecnologie per la tutela della salute e sicurezza dei lavoratori tra garanzie e vincoli*, in *Lavoro nella Giurisprudenza*, n. 6, 2021, pp. 591 ss.

Del Punta R., *La nuova disciplina dei controlli a distanza sul lavoro (art. 23 D. Lgsl. n. 151/2015)*, in *Rivista Italiana di Diritto del Lavoro (RIDL)*, vol. I, 2016, pp. 77 ss.
Dessì O., *Il controllo a distanza sui lavoratori. Il nuovo art. 4 Stat. Lav.,* Edizioni scientifiche Italiane, Napoli 2017.
Donini A., *Tecniche avanzate di analisi dei dati e protezione dei lavoratori*, in *Diritto delle Relazioni Industriali (DRI)*, n. 1, 2018, pp. 222 ss.
Durante M., *Potere computazionale. L'impatto delle ICT*, in Diritto società e sapere*,* Meltemi, 2019.
Fabbri T., Mandreoli F., Martoglia R., Scapolan A. C., *Employee Attitudes and (Digital) Collaboration Data: A Preliminary Analysis in the HRM Field*, 28th International Conference on Computer Communication and Networks (ICCCN), n. 7, 2019. This work is supported by UniMoRe under the project "*Framing employee attitudes and digital work behaviors to support data-driven human resource management.*
Faioli M., *Data analytics, robot intelligenti e regolazione del lavoro*, in *Federalismi.it*, n. 9, 2022, pp. 149 ss.
Fantoni G., Cervelli G., Pira S., Trivelli L., Mocenni C., Zingone R., Pucci T., *Ecosistemi 4.0: imprese, società, capitale umano,* in *Quaderni Fondazione G. Brodolini*, Edizione Fondazione Giacomo Brodolini, Roma, 2017.
Florczak I., Wujczyk M., *The lie as a privacy protection measure*, in Addabbo T., Ales E., Curzi Y., Fabbri T., Rymkevich O., Senatori I., *Performance appraisal in modern employment relations. An interdisciplinary approach*, Palgrave Macmillan, Switzerland, 2020.
Fregni A., Giugni G., *Lo statuto dei Lavoratori*, Giuffrè Editore, Milano, 1971.
Gelbard R., Ramon-Gonen R., Carmeli A., Bittmann R. M., Talyansky R, *Sentiment analysis in organizational work: Towards an ontology of people analytics,* in *Wiley Expert Systems*, 2018.
Grandi M. Pera G., *Commentario breve allo Statuto dei lavoratori,* Cedam, Padova, 1985.
Grillo Pasquarelli F., *Gli strumenti di controllo a distanza dei lavoratori*, Relazione tenuta all'incontro di studio "Jobs Act *dopo 5 anni: un quadro aggiornato della giurisprudenza*", organizzato dalla SSM, Scandicci, 13 - 15 gennaio 2020.
Grugulis I., Vincent S., *Whose skill is it anyway? 'Soft' skills and polarization,* in *Work Employment & Society*, vol. 23, n. 4, 2009, pp. 597 ss.
Ingrao A. *Il controllo a distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata*, Cacucci Editore, Bari, 2018.
Ingrao A., *Il braccialetto elettronico tra privacy e sicurezza del lavoro*, in *Diritto delle Relazioni Industriali*, n.3/XXIX, 2019, pp. 895 ss.
Ingrao A., *Il potere di controllo a distanza sull'ozio telematico e il limite del diritto alla privacy del lavoratore*, in *Rivista Italiana di Diritto del Lavoro*, vol. 3, 2019, pp. 416 ss.
Mainardi S., *Rivoluzione digitale e diritto del lavoro*, in *Massimario di Giurisprudenza del Lavoro*, fasc. 2, 2020, pp. 341 ss.
Maio V., *Il regime delle autorizzazioni del potere di controllo del datore di lavoro ed i rapporti con l'art. 8 della legge n. 148/2011*, in Tullini P. (a cura di), *Controlli a distanza e tutela dei dati personali dei lavoratori,* Giappichelli Editore, Torino, 2017.
Mantelero A., *Big Data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo,* in *Diritto dell'Informazione e dell'Informatica*, n. 1, 2012, pp. 135 ss.
Marazza M., *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore), in Argomenti di Diritti del Lavoro (ADL),* vol. 21, n. 3, 2016, pp. 483 ss.
Marazza M., *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore)* in *WP CSDLE "Massimo D'Antona".it – 300/2016*, pp. 291 ss.
Maresca A. *Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 St. lav.*, in Tullini P. (a cura di) *Controlli a distanza e tutela dei dati personali del lavoratore*, Giappichelli Editore, Torino, 2017.

Maresca A., *Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 dello statuto dei lavoratori,* in *Rivista Italiana del Diritto del Lavoro (RIDL)*, vol. 1, 2016, pp. 513 ss.
Mazzotti M., *Per una sociologia degli algoritmi*, in Rassegna Italiana di Sociologia, n. 3-4, 2015.
Messori G., *Utilizzo di modelli statico-predittivi e data mining: il caso INPS e alcune guidelines operative*, in *Cyberlaws, 24 settembre 2018*.
Morel L., *Le droit à la déconnexion en droit français. La question de l'effectivité du droit au repos à l'ère du numérique, Labour & Law Issues (LLI)*, vol. 3, n. 2, 2018, pp. 1 ss.
Sartori A., *Il controllo tecnologico sui lavoratori*, Giappichelli Editore, Torino, 2020.
Schneider B., *The people make the place*, in *Personnel Psychology*, vol. 40, n. 3, 1987, pp. 437 ss.
Shrivastava S., Nagdev K., Rajesh A., *Redefining HR using people analytics: the case of Google,* in *Human Resource Management International Digest,* vol. 26, n. 2, 2018, pp. 3 ss.
Stizia A., Lopez B., *Le più avanzate modalità di controllo sul lavoratore: Machine Learning e Social Media,* in Pisani C., Proia G., Topo A. (a cura di), *Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro*, Giuffrè Editore, Milano 2022.
Stizia A., *Personal computer e controlli "tecnologici" del datore di lavoro nella giurisprudenza,* in *Argomenti di Diritto del Lavoro (ADL),* n. 3, 2017, pp. 804 ss.
Tebano L., *Lavoro, potere direttivo e trasformazioni organizzative*, Editoriale scientifica, 2020, p. 239.
Trojsi A., *Al cuore del nuovo art. 4, co. 2, St. Lav.: la delimitazione della fattispecie degli "strumenti utilizzati per rendere la prestazione lavorativa",* in *Rivista Italiana di Diritto del Lavoro*, vol. II, n. 2, 2017, pp. 310 ss.
Trojsi A., *Il diritto del lavoratore alla protezione dei dati personali*, Giappichelli Editore, Torino, 2013.
Trojsi A., *Potere informatico del datore di lavoro e controllo sui lavoratori, cinquant'anni dopo*, in *dirittifondamentali.it,* n. 2, 2020, pp. 1411 ss.
Trojsi A., *Controllo a distanza (su impianti e strumenti di lavoro) e protezione dei dati del lavoratore*, in *Variazioni su Temi di Diritto del Lavoro*, n. 4, 2016, pp. 667.
Tullini P. (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Giappichelli Editore, Torino 2017.
Tullini P., *Comunicazione elettronica, potere di controllo e tutela del lavoratore*, in *Rivista Italiana di Diritto del Lavoro*, vol. 1, 2009, pp. 323 ss.
Tullini P., *Il controllo a distanza attraverso gli strumenti per rendere la prestazione lavorativa. Tecnologia di controllo e tecnologie di lavoro: una distinzione possibile?,* in Tullini P. (a cura di) *Controlli a distanza e tutela dei dati personali dei lavoratori*, Giappichelli Editore, Torino, 2017.
Vallauri M. L., *È davvero incontenibile la forza espansiva dell'art. 4 dello statuto dei lavoratori?,* in *Rivista Italiana di Diritto del Lavoro*, vol. 3, 2008, pp. 718 ss.
Veneziani B., *Sub art. 4*, in Freni A. Giugni G. (diretto da), *Lo Statuto dei lavoratori. Commentario alla legge 20 maggio 1970, n. 300,* Giuffrè Editore, Milano, 1979.
Zoli C., Villa E., *Gli strumenti di registrazione degli accessi e delle presenze*, in *Controlli a distanza e tutela dei dati personali del lavoratore*, P. Tullini (a cura di), Giappichelli, Torino, 2017.

Capitolo 3

Adam-Prassl J.*, A thematic working paper for the annual conference of the European Centre of Expertise (ECE) in the field of labour law, employment and labour market policies: exploring ways to improve working conditions of platform workers: the role of EU labour law. Algorithmic management and the EU social acquis: opening the black box*, october 2020.
Adams-Prassl J., *What If Your Boss Was an Algorithm? Economic Incentives, Legal Challenges, and the Rise of Artificial Intelligence at Work*, in *Comparative Labor Law & Policy Journal 123*, vol. 41, n. 1, 2019, pp. 1 ss.

Ballestrero M. V., *Ancora sui rider. La cecità discriminatoria della piattaforma*, in *Labor*, n. 1, 2021, pp. 1 ss.
Barbera M, *Discriminazioni algoritmiche e forme di discriminazione*, in *Labour & Law Issues (LLI)*, vol. 7, n. 1, 2021, pp. I 1 – I 17.
Barocas S, Selbst A. D., *Big Data's Disparate Impact*, in *California Law Review*, vol. 104, n. 671, 2016, pp. 677 ss.
Bersin J., Chamorro-Premuzic T., *The case for hiring older workers*, in *Harvard Business Review* consultabile *online* https://hbr.org/2019/09/the-case-for-hiring-older-workers.
Bogen M., *All the Ways Hiring Algorithms Can Introduce Bias*, Harvard Business Review, May 2019, consultabile *online* https://hbr.org/2019/05/all-the-ways-hiring-algorithms-can-introduce-bias.
Bresciani I., *Le forme di controllo nello Statuto dei lavoratori: orientamenti giurisprudenziali e questioni di attualità,* in *Variazioni su Temi di Diritto del Lavoro*, fasc. 4, 2016, pp. 731 ss.
Buolamwini J., Gebru T., *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, in *Proceedings of Machine Learning Research*, vol. 81, 2018, pp. 77 – 91.
Carnovali S., *Profili delle politiche nazionali ed europee di contrasto alle discriminazioni multiple,* Rivista del Gruppo di Pisa consultabile su: https://www.gruppodipisa.it/images/rivista/pdf/Sara_Carnovali_-_Profili_delle_politiche_nazionali_ed_europee_di_contrasto_alle_discriminazioni_multiple.pdf
Caruso B., Zappalà L., *Un diritto del lavoro "tridimensionale": valori e tecniche di fronte ai mutamenti dei luoghi di lavoro*, in *Biblioteca '20 Maggio',* n. 1, 2021 (originariamente pubblicato su *WP CSDLE.it*. n. 439, 2021), pp. 151 ss.
Cataudella A., *Sub art. 8*, in Prospetti U. (a cura di) *Commentario dello Statuto dei lavoratori*, Giuffrè Editore, Milano, 1975.
Cooney S., *LinkedIn Tweaks Search Algorithm After Report Suggests Gender Bias*, 8.9.2016, consultabile su https://time.com/4484530/linkedin-gender-bias-search/.
Dagnino E., *Dalla fisica all'algoritmo: una prospettiva di analisi giuslavoristica*, ADAPT University Press, 2019.
Dagnino E., *People analytics: lavoro e tutele al tempo del management tramite big data*, in *Labour & Law Issues (LLI)*, vol. 3, n. 1, 2017, pp. I 1-31.
Durante M., *Potere computazionale. L'impatto delle ICT*, in *Diritto società e sapere,* Meltemi, 2019.
Faioli M., *Discriminazioni digitali e tutela giudiziaria su iniziativa delle organizzazioni sindacali*, in *Diritto delle Relazioni Industriali* (*DRI)*, n. 1, 2021, pp. 204 ss.
Gaudio G., *Algorithmic management, poteri datoriali e oneri della prova: alla ricerca della verità materiale che si cela dietro l'algoritmo* in *Labour & Law Issues (LLI)*, vol.6, n. 2. 2020, pp. 19 – 71.
Gaudio G., *Algorithmic management, sindacato e tutela giurisdizionale*, in *Diritto delle Relazioni Industriali (DRI),* n. 1, 2022, pp. 1 ss.
Giacomelli L., *Big brother is «*gendering*» you. Il diritto antidiscriminatorio alla prova dell'intelligenza artificiale: quale tutela per il corpo digitale?*, in *BioLaw Journal*, n. 2, 2019, pp. 269 ss.
Hacker P., *Teaching fairness to artificial intelligence: existing and novel strategies against algorithmic discrimination under EU law,* in *55 Common Market Law Review*, 2018, pp. 1143 ss.
Ingrao A., Donini A., *Algoritmi e lavoro*, in *Labour Law Community del 25 maggio 2022*, consultabile *online* https://www.labourlawcommunity.org/ricerca/algoritmi-e-lavoro/ .
Ingrao A., *I sistemi di feedback basati su rating e reviews tra controllo della prestazione lavorativa e divieto di decisioni automatizzate*, in Alessi C., Barbera M., Guaglianone L. (a cura di), *Impresa, lavoro e non lavoro nell'economia digitale*, Cacucci Editore, Bari, 2019.
Ingrao A., *Il controllo a distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata*, Cacucci Editore, Bari, 2018.

Ingrao A., *Riflessioni intorno alla partecipazione dei lavoratori nell'era dell'algoritmo, alla luce dell'accordo Just Eat-Takeaway.com*, in Mingione E., Scarpelli F., Giasanti L. (a cura di), *Lo Statuto dei lavoratori alla prova dell'oggi: Una rilettura critica da parte degli studiosi di nuova generazione,* Feltrinelli, Milano, 2022.
Kanoogo Y., *Addressing Bias in HR Algorithms*, in Medium (Mar. 18, 2020), consultabile *online* https://medium.com/@yashkanoongo/addressing-bias-in-hr-algorithms-2b0f9003ed64.
Kullmann M., *Discriminating job applicants through algorithmic decision-making,* in SSRN, 1 gennaio 2019, consultabile *online* https://ssrn.com/abstract=3373533.
Lo Faro A., *Algorithmic Decision Making e gestione dei rapporti di lavoro: cosa abbiamo imparato dalle piattaforme*, in *Federalismi.it* , n. 25, 2022, pp. 189 ss.
Maio V., *Il diritto del lavoro e le nuove sfide della rivoluzione robotica*, in *Argomenti di Diritto del Lavoro (ADL)*, n. 6, 2018, pp. 1414 ss.
Mazzotta O., *Diritto del lavoro*, Giuffrè Editore, Milano, 2011.
McKenzie R., *Bots, Bias and Big Data: Artificial Intelligence, Algorithmic Bias and Disparate Impact Liability in Hiring Practices*, in *Arkansas Law Review*, vol. 71, n. 2, 2018, pp. 529 ss.
Melendez S., *Uber driver troubles raise concerns about transgender face recognition*, 8.9.2018*,* consultabile su *https://www.fastcompany.com/90216258/uber-face-recognition-tool-has-locked-out-some-transgender-drivers.*
Militello M. – Strazzari D., *I fattori di discriminazione*, in M. Barbera - A. Guariso (a cura di), *La tutela antidiscriminatoria*, Giappichelli Editore, Torino, 2019.
Mitchell T., *The need for biases in learning generalizations*, Rutgers University, 1980.
Molaschi V., *Algoritmi e nuove schiavitù*, in *Federalismi.it,* n. 18, 2021, pp. 205 ss.
Nardocci C., *Intelligenza artificiale e discriminazion*e, in atti del Convegno annuale Associazione Gruppo di Pisa "*Il diritto costituzionale e le sfide dell'innovazione tecnologica",* Genova 18/19 giugno 2021.
Pajno A., Bassini M.,De Gregorio G., Macchia M., Patti F. P.., Pollicino O., Quattrocolo S., Simeoli D., Sirena P., *AI: profili giuridici. Intelligenza artificiale: criticità emergenti e sfide per il giurista*, in *BioLaw Journal*, n. 3, 2019, pp. 205 ss.
Pasquale F., *The black box society: the secret algorithms that control money and information*, Cambridge Mass., Harvard University Press, London, 2016.
Pera G., *Sub art. 8,* in Assanti C., Pera G. (a cura di), *Commento allo statuto dei diritti dei lavoratori*, Cedam, Padova, 1972.
Perulli A., *La discriminazione algoritmica: brevi note introduttive a margine dell'Ordinanza del Tribunale di Bologna,* in Lavoro Diritti Europa, 14 gennaio 2021 (https://www.lavorodirittieuropa.it/dottrina/lavori-atipici/644-la-discriminazione-algoritmica-brevi-note-introduttive-a-margine-dell-ordinanza-del-tribunale-di-bologna).
Perulli A., *La discriminazione algoritmica: brevi note introduttive a margine dell'Ordinanza del Tribunale di Bologna*, in *Lavoro Diritti Europa*, n. 1, 2021, pp. 1 ss.
Peruzzi M., *Il diritto antidiscriminatorio al test di intelligenza artificiale*, in *Labour & Law Issues (LLI)*, vol. 7, n.1, 2021, pp. I 48 – I 76.
Pignatiello G., *Il contrasto alle discriminazioni algoritmiche*, in *Federalismi.it*, n. 16, 2021, pp. 164 ss.
Purificato I., Senatori I., *The Position of Collective Rights in the "Platform Work" Directive Proposal: Commission v Parliament*, in *Hungarian Labour Law E- Journal*, 2023/1, pp. 1 ss.
Rodotà S., *Il mondo nella rete. Quali i diritti, quali i vincoli*, Laterza, Roma-Bari, 2014
Santagata De Castro R., *Anti- discrimination Law in the Italian Courts: the new frontiers of the topic in the age of algorithms*, in *Biblioteca '20 Maggio'*, n. 1, 2021 (originariamente pubblicato in *WP CSDLE.it,* n. 440, 2021), pp. 193 ss.
Serra B. G., *Le schedature Fiat. Cronaca di un processo e altre cronache*, Rosenberg & Sellier, Torino,1994.

Simoncini A., *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal*, n. 1, 2019, pp. 63 ss.
Spencer J., *Age and Disability Discrimination & Your Rights*, su Jackson Spencer Law del 5 Mar. 2020, consultabile *online* https://jacksonspencerlaw.com/age-and-disability-discrimination/
The Coded Gaze: https://www.ajlunited.org/the-coded-gaze.
The New York Times, *We need laws to take on racism and sexixm in hiring technology*, consultabile *online* https://www.nytimes.com/2021/03/17/opinion/ai-employment-bias-nyc.html.
Timellini C., *Le condotte social dei lavoratori sotto la lente della giurisprudenza*, in *Argomenti di Diritto del Lavoro (ADL),* n. 1, 2020, pp. 283 ss.
Tommasi S., *Algoritmi e nuove forme di discriminazione: uno sguardo al diritto europeo,* in *Revista de Direito Brasileira*, vol. 27, n. 10, 2020, pp. 112 ss.
Trojsi A., *Controllo a distanza (su impianti e strumenti di lavoro) e protezione dei dati del lavoratore*, in *Variazioni su Temi di Diritto del Lavoro*, n. 4, 2016, pp. 667.
Trojsi A., *Potere informatico del datore di lavoro e controllo sui lavoratori, cinquant'anni dopo*, in *dirittifondamentali.it,* n. 2, 2020, pp. 1411 ss.
Tullini P., *La salvaguardia dei diritti fondamentali della persona che lavora nella gig-economy*, in *Costituzionalismo.it*, n.1, 2020, pp. 39 ss.
Vespignani A., Rijtano R., *L'algoritmo e l'oracolo. Come la scienza predice il futuro o ci aiuta a cambiarlo*, il Saggiatore, Milano, 2019.
Wickens C.D, Clegg B.A., Vieane A.Z, Sebok A.L., *Complacency and Automation Bias in the Use of Imperfect Automation*, in *Human factors*, vol. 57, n. 5, 2015, pp. 728 ss.
Zuddas P., *Intelligenza Artificiale e discriminazioni,* in Consulta *OnLine*, 16 marzo 2020, pp. 1 ss.

Capitolo 4

Carinci M. T., Giudici S., Perri P., *Obblighi di informazione e sistemi decisionali e di monitoraggio automatizzati (art. 1-bis "Decreto Trasparenza"): quali forme di controllo per i poteri datoriali algoritmici?,* in *Labor*, n. 1, 2023, pp. 7 ss.
Faioli M., *Trasparenza e monitoraggio digitale. Perché abbiamo smesso di capire la norma sociale europea*, in *Federalismi.it*, n. 25, 2022, pp.104 ss.
Ingrao A., *Il controllo a distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata,* Cacucci, Bari, 2018.
Manganaro F., *Trasparenza e digitalizzazione*, in *Diritto e processo amministrativo*, n. 1, 2019, pp. 25 ss.
Otranto P., *Riflessioni in tema di decisione amministrativa, intelligenza artificiale, legalità,* in *Federalismi.it*, n. 7, 2021, pp. 187 ss.
Ricci M., Olivieri A. (a cura di), *La tutela dei dati del lavoratore. Visibile e invisibile in una prospettiva comparata,* Cacucci, Bari, 2022.
Rossilli B., *Obblighi informativi relativi all'utilizzo di sistemi decisionali e di monitoraggio automatizzati indicati nel decreto "Trasparenza"*, in *Federalismi.it*, Focus lavoro persona tecnologia. Paper del 5 ottobre 2022, pp. 1 ss.
Simoncini A., *L'algoritmo incostituzionale: intelligenza artificiale e futuro delle libertà*, in *BioLaw*, n. 1, 2019, pp. 63 ss.
Sitzia A., *Il diritto alla "privatezza" nel rapporto di lavoro tra fonti comunitarie e nazionali*, Cedam, Padova, 2013.
Tullini P. (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore,* Giappichelli Editore, Torino, 2017.
Tullini P. (a cura di), Web *e lavoro. Profili evolutivi e di tutela,* Giappichelli Editore, Torino, 2017.

Capitolo 5 e Note conclusive

Abraha H., Adams-Prassl J., Kelly Lyth A., *Finetuning the EU's Platform Work Directive*, in *Oxford Business Law Blog*, del 17 maggio 2022, disponibile al *link* https://blogs.law.ox.ac.uk/business-law-blog/blog/2022/05/finetuning-eus-platform-work-directive.

Abriani N., Schneider G., *Diritto delle imprese e intelligenza artificiale. Dalla Fintech alla Corptech*, il Mulino, Bologna, 2021.

Adams Prassl J., *Regulating Algorithms at Work: Lessons for a 'European Approach to Artificial Intelligence'*, in *European Labour Law Journal*, vol. 13, n. 1, 2022, consultabile al *link* https://journals.sagepub.com/doi/full/10.1177/20319525211062558.

Alaimo A., *Il pacchetto di misure sul lavoro nelle piattaforme: dalla proposta di Direttiva al progetto di Risoluzione del Parlamento europeo. Verso un incremento delle tutele?*, in *Labour & Law Issues (LLI),* vol. 8, n. 1, 2022, R.1- R.28.

Alaimo A., *Il Regolamento sull'Intelligenza Artificiale,* in *Federalismi.it*, n. 25, 2023, pp. 132 ss.

Alaimo A., *L'eterno ritorno della partecipazione: il coinvolgimento dei lavoratori al tempo delle nuove regole sindacali*, in *Biblioteca 20 Maggio,* 2/2014 (Originariamente pubblicato come WP C.S.D.L.E. "Massimo D'Antona".IT – 219/2014), pp. 1 ss.

Alaimo A., *Lavoro e piattaforme tra subordinazione e autonomia: la modulazione delle tutele nella proposta della Commissione europea*, in *Diritto delle Relazioni Industriali*, n. 2, 2022, pp.639 ss.

Ales E., Bel M., Deinert O., Robin-Olivier S. (a cura di), *International and European Labour Law: Article-by-Article Commentary*. London, Beck Hart Nomos, 2018.

Aloisi A., Gramano E., *Artificial intelligence is watching you at work: digital surveillance, employee monitoring, and regulatory issues in the Eu context,* in *Special Issue of Comparative Labor Law & Policy Journal, "Automation, Artificial Intelligence and Labour Protection",* edited by Valerio De Stefano, Vol. 41, n. 1, pp. 95 ss.

Armaroli I, Dagnino E., *A Seat at the Table: Negotiating Data Processing in the Workplace*, in *Comparative Labour Law & Policy Journal*, vol. 41, n. 1, 2019, pp. 173-195.

Astone A., *Autodeterminazione nei dati e sistemi A.I.*, in *Contratto e impresa*, n. *2.*, 2022, pp. 429 ss.

Barbieri M., *Prime osservazioni sulla proposta di direttiva per il miglioramento delle condizioni di lavoro nel lavoro con piattaforma*, in *Labour & Law Issues (LLI),* vol. 7, n. 2, 2022, C1-C.20.

Bergamaschi S., *Il ruolo dei Dati nella trasformazione della società*, in *Lavoro Diritti Europa*, n. 3, 2022.

Biasi M., *Il nodo della partecipazione dei lavoratori in Italia*, Egea, 2013; Frosecchi G., *Diritti collettivi di informazione. Lezioni dal caso GKN,* in *Labour & Law Issues*, vol. 7, n. 2, 2021, pp. 43, 44.

Bossen C., Dindler C., Iversen S. O., *Evaluation in participatory design: a literature survey*, in *Proceedings of the 14th Participatory Design Conference*, vol.1, 2016, pp. 151-160.

Cappellazzo N., *L'art. 8 Stat. Lav. e i meccanismi di HR algorithms management: lo Statuto dei lavoratori alla prova delle nuove tecnologie*, in *Federalismi.it* del 9 agosto 2023, n. 21/2023, pp. 187 ss.

Carinci M. T., Giudici S., Perri P., *Obblighi di informazione e sistemi decisionali e di monitoraggio automatizzati (art. 1-bis "Decreto Trasparenza"): quali forme di controllo per i poteri datoriali algoritmici?,* in *Labor*, n. 1, 2023, pp. 7 ss.

Corti M. *Il coinvolgimento dei lavoratori preso sul serio: il caso GKN,* in *Diritto delle Relazioni Industriali (DRI),* n. 1, 2022, pp. 265 ss.

Corti M., *Potere di controllo e nuove tecnologie. Il ruolo dei partner sociali,* in *Labour & Law Issues (LLI),* vol. 9, n.1, 2023, pp. I 59 ss.

Covelli R., *Lavoro e intelligenza artificiale: dai principi di trasparenza algoritmica al diritto alla conoscibilità*, in *Labour & Law Issues (LLI),* vol. 9, n. 1, 2023, pp. I 77 ss.

Crisafulli V., Paladin L., *Commentario breve alla Costituzione,* Cedam, Padova, 1990.

D'Antona M., *L'art. 4 dello Statuto dei Lavoratori ed elaborati elettronici*, in De Luca-Tamajo R., Imperiali-D'Afflitto R., Pisani. C., Romei R. (a cura di), *Nuove tecnologie e tutela della riservatezza del lavoratore*, Giuffrè Editore, Milano, 1988.

Dagnino E., *Dalla fisica all'algoritmo: una prospettiva di analisi giuslavoristica*, Adapt University Press, 2019.
De Luca Tamajo R., *La norma inderogabile nel diritto del lavoro*, Editore Jovene, Napoli, 1976.
De Stefano V., *'Masters and Servers': Collective Labour Rights and Private Government in the Contemporary World of Work*, in *International Journal of Comparative Labour Law and Industrial Relations*, vol. 36, n. 4, 2020, pp. 425-444.
De Stefano V., *Negotiating the Algorithm: Automation, Artificial Intelligence and Labour Protection*, in *Comparative Labor Law & Policy Journal,* vol. 41, n. 1, pp. 1 ss.
De Stefano V.; *The EU Commission's proposal for a Directive on Platform Work: an overview;* in *Italian Labour Law e-Journal,* n. 1, vol. 15, 2022, pp. 1 ss.
Delfino M., *Lavoro mediante piattaforme digitali, dialogo sociale europeo e partecipazione sindacale*, in *Federaslismi.it*, n. 25, 2023, pp. 170 ss.
Dessì O., *Il controllo a distanza sui lavoratori. Il nuovo art. 4 Stat. lav.,* Edizioni Scientifiche Italiane, Napoli, 2017, pp. 175-177.
Donini A, *Piattaforme*, in Novella M., Tullini P. (a cura di), *Lavoro digitale*, Giappichelli Editore, 2022, pp. 25-45.
Fabbri T., Mandreoli F., Martoglia R., Scapolan A. C., *Employee Attitudes and (Digital) Collaboration Data: A Preliminary Analysis in the HRM Field*, 28th International Conference on Computer Communication and Networks (ICCCN), n. 07 2019. This work is supported by UniMoRe under the project "*Framing employee attitudes and digital work behaviors to support data-driven human resource management*".
Fabris P., *L'indisponibilità dei diritti dei lavoratori*, Giuffrè Editore, Milano, 1978.
Faioli M., *Trasparenza e monitoraggio digitale. Perché abbiamo smesso di capire la norma sociale europea*, in *Federalismi.it*, del 5 ottobre 2022, n. 25, pp. 104 – 115.
Faleri C., *Asimmetrie informative e tutela del prestatore di lavoro*, Giuffrè Editore, Milano, 2007
Faleri C., *Brevi spunti di riflessione sull'evoluzione delle relazioni sindacali nell'economia digitale*, in *IANUS*, n. 24, 2021, pp. 93 ss.
Frosecchi G., *Diritti collettivi di informazione. Lezioni dal caso GKN,* in *Labour & Law Issues (LLI*), vol. 7, n. 2, 2021, pp. 37 ss.
Gambino A.M., Stazi A. (a cura di), *La circolazione dei dati. Titolarità, strumenti negoziali, diritti e tutele,* Pacini Giuridica, Pisa, 2020.
Garofalo D., *Prefazione,* in Zilli A., *La trasparenza nel lavoro subordinato. Principi e tecniche di tutela*, Pacini Giuridica, 2022.
Gunning D., *Explainable artificial intelligence (xAI)*, in *Technical Report, Defense Advanced Research Projects Agency* (DARPA), 2017, pp. 44 ss.
Imberti L., *La contrattazione collettiva aziendale di fronte alle sfide della rivoluzione digitale e ai processi di cambiamento organizzativo*, in *Federalismi.it*, n. 25, 2022, pp. 160 ss.
Ingrao A., *Controllo a distanza e privacy del lavoratore alla luce dei principi di finalità e proporzionalità della sorveglianza*, in *Labour & Law Issues (LLI),* vol. 9, n. 1, 2023, pp. I 102 ss.
Ingrao A., *Data-driven management e strategie collettive di coinvolgimento dei lavoratori per la tutela della privacy*, in *Labour & Law Issues* (LLI), vol. 5, n. 2, 2019, pp. 127–143.
Ingrao A., *Il controllo a distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata*, Cacucci Editore, Bari, 2018.
Ingrao A., *Riflessioni intorno alla partecipazione dei lavoratori nell'era dell'algoritmo, alla luce dell'accordo Just Eat-Takeaway.com*, in Mingione E., Scarpelli F., Giasanti L. (a cura di), *Lo Statuto dei lavoratori alla prova dell'oggi: Una rilettura critica da parte degli studiosi di nuova generazione,* Feltrinelli, Milano, 2022.
Iodice R., *La proposta di Regolamento UE sull'Intelligenza Artificiale: quali implicazioni sul versante giuslavoristico?,* in *IANUS*, n. 24, 2021, pp. 55 ss.

Lamberti F., *La proposta di regolamento UE sull'Intelligenza Artificiale alla prova della privacy*, in *Federalismi.it*, del 29 giugno 2022, pp. 1 ss.
Lo Faro A., *Algorithmic Decision Making e gestione dei rapporti di lavoro: cosa abbiamo imparato dalle piattaforme*, *in Federalismi.it*, n.25, 2022, pp. 201 ss;
Lo Sapio G., *La trasparenza sul banco di prova dei modelli algoritmici,* in *Federalismi.it*, n. 11, 2021, pp. 238 ss.
Loi P., *Il rischio proporzionato nella proposta di regolamento sull'IA e i suoi effetti nel rapporto di lavoro*, in *Federalismi.it,* n.4, 2023, pp. 239 ss.
Maio V., *Il regime delle autorizzazioni del potere di controllo del datore di lavoro ed i rapporti con l'art. 8 della legge n. 148/2011,* in Tullini P. (a cura di), *Controlli a distanza e tutele dei dati personali del lavoratore*, Giappichelli Editore, Torino, 2017.
Manafi Varkiani S., Pattarin F., Fabbri T., Fantoni G., *Predicting Employee Attrition by Machine Learning*, Conference Paper, Conference: 2021 4th International Conference on Artificial Intelligence and Big Data (ICAIBD), May 2021.
Natali L. C., *Intelligenza artificiale e impatto sul lavoro, in Diritto e Pratica del Lavoro,* n. 23, 1° giugno 2023, pp. 1446 ss.
Nicotra I., *Privacy vs trasparenza, il Parlamento tace e il punto di equilibrio lo trova la Corte*, in *Federalismi.it*, n. 7, 2019, pp. 1 ss.
Otto M., *A step towards digital self- & co-determination in the context of algorithmic management systems*, in *Italian Labour Law e-Journal*, 2022, 2, p. 51 ss.
Peruzzi M., *Intelligenza Artificiale e lavoro. Uno studio su poteri datoriali e tecniche di tutela,* Giappichelli Editore, Torino, 2023.
Piccinini I., Isceri M., *IA e datori di lavoro: verso una e-leadership?,* in *Lavoro Diritti Europa*, n. 2, 2021, pp. 1 ss.
Poletti D., *Gli intermediari dei dati*, in *European Journal of Privacy Law & Technologies*, n. 1, 2022, pp. 45 ss.
Purificato I., Senatori I., *The Position of Collective Rights in the 'Platform Work' Directive Proposal: Commission v Parliament*, in *Hungarian Labour Law E-Journal*, n. 1, 2023, pp. 1 ss.
Recchia G. A., *Condizioni di lavoro trasparenti, prevedibili e giustiziabili*, in *Labour & Law Issues (LLI),* vol. 9, n. 1, 2023, pp.C.33 ss.
Rota, A., *Sull'Accordo quadro europeo in tema di digitalizzazione del lavoro*, in *Labour & Law Issues (LLI)*, vol. 6, n. 2, 2020, pp. C.23-C.48.
Rudin V. C., *Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead,* in *Nat Mach Intell*, n. 1, 2019.
Sartori A., *Il controllo tecnologico sui lavoratori. La nuova disciplina italiana tra vincoli sovranazionali e modelli comparati*, G. Giappichelli Editore, Torino, 2020.
Scagliarini S., *La tutela della privacy e dell'identità personale nel quadro dell'evoluzione tecnologica,* in *Consulta OnLine*, n. 2, 2021, pp. 489 ss.
Senatori I., *Regulating the Employment Relationship in the Organization 4.0: Between Social Justice and Economic Efficiency*, in Perulli A., Treu T. (a cura di) *The Future of Work. Labour Law and Labour Market Regulation in the Digital Era*, Wolters Kluwer, Paesi Bassi, 2021.
Senatori, I., *The European Framework Agreement on Digitalisation: a Whiter Shade of Pale*?, in *Italian Labour Law e-Journal*, 13(2), 2020, pp. 159-175.
Smuraglia C., *Progresso tecnico e tutela della personalità del lavoratore*, in Rivista Giuridica del Lavoro, Vol. 1, 1960.
Spinelli C., *Il regolamento (UE) 2022/868 sulla governance dei dati e le sue possibili ricadute sulle misure di inclusione lavorativa delle persone con disabilità*, in Federalismi.it, n. 9, 2023, pp. 257 ss.
Spinelli C., *La trasparenza delle decisioni algoritmiche nella proposta di Direttiva UE sul lavoro tramite piattaforma*, in *Lavoro Diritti Europa*, n. 2, pp. 6 ss.

Tebano L, *Fabbrica 4.0 e potere di "controllo direttivo"*, in Rusciano M., Gaeta L., Zoppoli L. (a cura di), *Mezzo secolo dallo statuto dei lavoratori*, in *Quaderni della Rivista Diritti Lavori Mercanti,* n. 8, 2020, pp. 443 ss.
Tebano L, *Lavoro, potere direttivo e trasformazioni organizzative,* Editoriale Scientifica, Napoli, 2020.
Tebano L., *La digitalizzazione del lavoro tra intelligenza artificiale e gestione algoritmic*a; in *IANUS*, n. 24, 2021, pp. 42 ss.
Topo A., *Circolazione di informazioni, dati personali, profilazione e reputazione del lavoratore*, in Pisani C., Proia G., Topo A. (a cura di), *Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro*, Giuffrè Editore, Milano, 2022, pp. 389 ss.
Topo A., Tardivo D., *Hard law e soft law nel diritto dell'Unione europea in materia di trattamento dei dati personali e di tutela della riservatezza del lavoratore*, in Pisani C., Proia G., Topo A. (a cura di), *Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro*, Giuffrè Editore, Milano, 2022.
Treu T., *La digitalizzazione del lavoro: proposte europee e piste di ricerca*, in *Federalismi.it,* n. 9, 2022, p. 190 ss.
Trojsi A*, Sull'impatto giuslavoristico del Data Governance Act. Riflessioni sistemiche a prima lettura del Regolamento (UE) 2022/868*, in *Federalismi.it*, n. 4, 2022, pp. 276 ss.
Tullini P., *Il controllo a distanza attraverso gli strumenti per rendere la prestazione a distanza*, in Tullini P. (a cura di) *Controlli a distanza e tutele dei dati personali del lavoratore*, G. Giappichelli Editore, Torino, 2017, pp. 123 ss.
Tullini P., *La Direttiva Piattaforme e i diritti del lavoro digitale,* in *Labour & Law Issues (LLI), vol. 8, n. 1,*2022, R 43 – R 56.
Tullini P., *La nuova proposta europea sull'intelligenza artificiale e le relazioni di lavoro*, in *Trabajo, Persona, Derecho, Mercados,* n. 5, 2022, pp. 99-108.
Wachter S., Mittelstadt B., Russell C., *Counterfactual explanations without opening the black box: automated decisions and the GDPR,* in *Harvard Journal of Law & Technology* Vol. 31, n. 2 Spring 2018, pp. 861 ss.
Zappalà L., *Appunti su linguaggio, complessità e comprensibilità del lavoro 4.0: verso una nuova procedimentalizzazione dei poteri datoriali*, in *WP CSDLE "Massimo D'Antona"*.it, n. 462, 2022, pp. 1 ss.
Zappalà L.; *Algoritmo*, in Borelli S, Brino V., Faleri C., Lazzeroni L, Tebano L., Zappalà L., *Lavoro e tecnologie. Dizionario del diritto del lavoro che cambia,* Giappichelli Editore, Torino, 2022, pp. 17 ss.
Zilli A., *La trasparenza nel lavoro subordinato. Principi e tecniche di tutela*, Pacini Giuridica, 2022, p. 66, Libro in Open Access scaricabile gratuitamente dall'archivio IRIS – Anagrafe della ricerca https://air.uniud.it/.
Zoppoli L., *Modelli partecipativi e tecniche di regolazione dei rapporti di lavoro*, in *Diritto delle Relazioni Industriali (DRI),* vol. 20, n. 1, 2010, pp. 19 ss.