Mara Parpaglioni

INTELLIGENZA ARTIFICIALE NEI LUOGHI DI LAVORO: NUOVE FRONTIERE DEL DIRITTO E SFIDE SINDACALI

1. *Per la costruzione di un rapporto di fiducia tra lavoratori e IA*

L'IA e, più in generale, i software basati su algoritmi applicati agli strumenti di lavoro sono oramai talmente diffusi che l'interazione tra lavoratore e software è una realtà estesa alla quasi totalità dei processi produttivi e coinvolge in ugual modo sia operai che impiegati. Tale fenomeno è poi notevolmente cresciuto a seguito della recente emergenza sanitaria, durante la quale si è avuta un'accelerazione del ricorso a forme di lavoro a distanza o mediante l'utilizzo di piattaforme digitali[1], che con ogni probabilità, anche dopo tale periodo, rimarranno come una delle normali forme di lavoro.

Se da un lato l'applicazione al lavoro di tali tecnologie, grazie alle quali la prestazione può essere resa in ogni luogo e in qualsiasi momento, ha reso possibile continuare a lavorare anche nell'emergenza, nello stesso tempo tale fenomeno però ha comportato una sempre maggiore frammentazione e decentramento del lavoro sia nella sua organizzazione che nell'esecuzione spazio-temporale, creando un modello produttivo che isola sempre più i lavoratori dai colleghi e dalle organizzazioni sindacali. Ciò è avvenuto non solo in quelle realtà produttive nelle quali ai lavoratori non viene

Cap. XVI di: ASTRID, *Intelligenza artificiale e diritto: una rivoluzione?*, vol.I, Il Mulino, 2022

[1] Sull'impatto dell'emergenza sanitaria causata dall'epidemia da COVID-19 sul mondo del lavoro, cfr. A. Maresca, *Il diritto del lavoro al tempo del COVID-19*, in «Federalismi», 2020, pp. 8 ss.; A Pileggi (a cura di), *Il diritto del lavoro dell'emergenza epidemiologica*, Roma, 2020; O. Bonardi, U. Carabelli, M. D'Onghia e L. Zoppoli, *Covid 19 e diritti dei lavoratori*, Roma, 2020.

neppure riconosciuto lo *status* di dipendente (cfr. il fenomeno dei cd. rider), ma anche all'interno del rapporto di lavoro tradizionalmente subordinato.

Questo «effetto grotta» che «divide» e «isola» i lavoratori, indebolendo la consapevolezza e la salvaguardia dei propri diritti anche in termini di salute e di sicurezza nei luoghi di lavoro, oltre ad avere conseguenze sull'aumento dello stress da videoterminali per iperconnettività e sulle patologie muscolo-scheletriche a causa del sovrapporsi dei tempi di vita e di lavoro, costituisce una forma di nuova alienazione[2]. Con la conseguenza che, anziché portare a risultati di maggiore efficienza, rischia di produrre un depauperamento della stessa società civile, poiché l'isolamento e l'impoverimento relazionale e dei diritti impedisce quella crescita personale e sociale all'interno dei luoghi di lavoro dove dovrebbe trovare libera esplicazione la personalità del lavoratore.

Deve quindi essere valutato con ponderata attenzione un utilizzo indiscriminato delle potenzialità offerte dall'IA di controllare in modo invasivo, penetrante e occulto il lavoratore, così come di poterlo «contattare» in ogni momento e in ogni luogo. Una tale organizzazione del lavoro non può di certo accrescere né il benessere del lavoratore, né la produttività, ove non si riesca a introdurre sistemi che permettano di conciliare i tempi di vita con quelli di lavoro e le potenzialità offerte da tali tecnologie con la salvaguardia dei diritti dei lavoratori. Affinché possa sorgere una nuova era della produzione e del lavoro e con essa della società tutta, dovrà costituirsi un patto di fiducia tra lavoratore e IA che non potrà realizzarsi se l'introduzione di queste nuove tecnologie si tradurrà in una perdita di tutele e di garanzie per i lavoratori.

Attualmente l'organizzazione del lavoro sta prendendo strade che si allontanano da tale obiettivo e pertanto è necessaria una riflessione su un impiego «etico» dell'IA e degli algoritmi per costruire un rapporto di trasparenza e di garanzie per i lavoratori.

[2] S. Gheno e L. Pesenti, *Smart working: una trasformazione da accompagnare*, in «Lavoro Diritti Europa», 2021, n. 1, p. 11 dell'estratto.

Il rischio infatti è che si realizzi una nuova organizzazione del lavoro basata sull'impiego dell'IA nella quale il datore di lavoro sostituisca il potere direttivo e di controllo (come regolato e limitato dalle norme di legge vigenti) con un suo «ologramma tecnologico» molto più invasivo, penetrante e spesso occulto, che si presenta come un «asettico» strumento di lavoro, ma che invece è in grado di impartire disposizioni anche molto dettagliate, verificare l'esecuzione della prestazione oltre che il risultato e valutare non solo il rendimento, ma tutta l'attività lavorativa e anche il comportamento tenuto fuori dall'orario di lavoro (come ad es. tramite il monitoraggio dei social network).

L'introduzione dell'IA e di software nell'organizzazione del lavoro sta creando nuove vulnerabilità dei diritti che si ritenevano oramai definitivamente acquisiti, come la tutela della dignità umana, della protezione dei dati personali, della identità personale, nonché il diritto alla non discriminazione, alla salute e alla sicurezza nei luoghi di lavoro.

Tali tecnologie infatti incidono sul divieto di controllo a distanza dei lavoratori sancito dall'art. 4, l. 300/1970 rendendolo sempre più evanescente e meno trasparente. Nelle nuove forme e modalità di lavoro, infatti, il concetto di strumento di lavoro e quello di strumento di controllo tendono a sovrapporsi; occorre, quindi, ribadire la necessità di limitare tale controllo, anche là dove la prestazione viene resa nelle modalità del lavoro agile o del telelavoro con l'utilizzo di nuove tecnologie che servono ai lavoratori per rendere la prestazione e ai datori di lavoro per controllare i propri dipendenti.

Oggi infatti non si discute più di apparecchiature «aggiuntive» (telecamere o microfoni occulti), ma sono le stesse modalità ordinarie del collegamento in rete (non solo durante il lavoro e non solo nello *smart working*) a creare collegamenti permanenti ad alta invasività.

Secondo il nuovo testo dell'art. 4, l. 300/1970, si può affermare che rientrano nella categoria degli strumenti utilizzati dal lavoratore per rendere la prestazione e ai quali non si applica la procedura dell'accordo sindacale o, in subordine, quella amministrativa: il computer, la posta elettronica e l'ac-

cesso a internet. Ma così non è nel caso in cui a tali strumenti vengano installati software o algoritmi che consentono di monitorare l'attività svolta dal lavoratore, addirittura utilizzando algoritmi di profilazione ai fini di valutarne il rendimento, in quanto sicuramente non necessario per rendere la prestazione. Anche se l'installazione del computer o dello smartphone di per sé non richiede l'autorizzazione preventiva sindacale o amministrativa, in caso di installazione di software a questi strumenti diventa successivamente necessaria[3].

A ciò si aggiunga che il nuovo scenario reso possibile dall'IA e dagli algoritmi impiegati nel contesto lavorativo ha già fatto nascere nuove o diverse forme di lavoro che tendono a mistificare il rapporto di lavoro subordinato, in quanto non più riconducibile interamente e completamente ai parametri già conosciuti dalla dottrina e dalla giurisprudenza di settore.

Tali problematiche sono infatti oggigiorno già presenti non solo nel lavoro agile, o comunque svolto a distanza, ma anche in tutti quei settori nei quali l'attività lavorativa, per sua intrinseca natura, deve essere svolta al di fuori dei locali aziendali e dove quindi l'interesse al controllo da parte del datore di lavoro è maggiormente sentito. Emblematico in tal senso è il settore della logistica di cui tanto si è parlato di recente con riferimento alla vicenda dei cd. rider[4], sia con riferimento alle modalità con le quali vengono trattati i dati dei lavoratori da parte di tali piattaforme[5], sia in merito

[3] D'altra parte, in tal senso si è espresso sia il Garante per la protezione dei dati personali, con il provvedimento del 13/7/2016, n. 303, sia il ministero del Lavoro e delle politiche sociali con la nota del 18/6/2015.

[4] Crescente attenzione sta suscitando anche il modello economico di Uber e il rapporto di lavoro dei suoi autisti, su cui cfr. A. Belloni, *Uberization. Il potere globale della disintermediazione*, Milano, 2017; A. Perulli, *Lavoro e tecnica al tempo di Uber*, in «Rivista giuridica del lavoro e della previdenza sociale», 2017, n. 21, pp. 195 ss.

[5] Il Garante della privacy italiano, attivata una procedura congiunta di cooperazione europea con la Spagna, ha comminato alla società Foodinho una sanzione di 2,6 milioni di euro per illegittimità del trattamento dei dati dei rider effettuato tramite la propria piattaforma digitale, in quanto gli algoritmi utilizzati per il suo funzionamento sono stati valutati discriminatori e lesivi dei diritti degli interessati sanciti

a problematiche relative alla configurabilità o meno di un rapporto di lavoro subordinato mediato dal software che di fatto gestisce tutta l'attività lavorativa[6].

E così si giunge a un apparente paradosso: da un lato queste stesse tecnologie svincolano il lavoratore dal coordi-

anche dallo statuto dei lavoratori, oltre che della recente normativa a tutela di chi lavora con le piattaforme digitali. In particolare, la società, ad esempio, non aveva adeguatamente informato i lavoratori sul funzionamento del sistema e non assicurava garanzie sull'esattezza e la correttezza dei risultati dei sistemi algoritmici utilizzati per la valutazione dei rider. Non garantiva nemmeno procedure per tutelare il diritto di ottenere l'intervento umano, esprimere la propria opinione e contestare le decisioni adottate mediante l'utilizzo degli algoritmi in questione, compresa l'esclusione di una parte dei rider dalle occasioni di lavoro. Il Garante italiano ha anche attivato, per la prima volta, una operazione congiunta di cooperazione europea, ai sensi del GDPR, con il Garante spagnolo per verificare il funzionamento della piattaforma digitale di proprietà della capogruppo GlovoApp (cfr. Registro dei provvedimenti n. 234 del 10/6/2021 - doc. web n. 9675440).

[6] La Cassazione con la sentenza n. 1663/2020 del 24/1/2020 ha confermato che i rider vanno tutelati come lavoratori subordinati, respingendo il ricorso di Foodinho, nel contenzioso tra Foodora e cinque rider di Torino. Per la Suprema Corte, ai ciclofattorini delle consegne a domicilio vanno applicate le tutele del lavoro subordinato, come previsto dal *Jobs Act*, nella forma «ibrida» delle «collaborazioni organizzate dal committente, con condanna della Foodinho al pagamento delle differenze retributive e dei contribuiti previdenziali non versati, con riferimento al quinto livello del contratto collettivo logistica-trasporto; cfr. anche Trib. Milano, sez. in part. Impresa, 9/7/2015, commentata da A. Donini, *Regole della concorrenza e attività di lavoro nella «on demand economy»: brevi riflessioni sulla vicenda Uber*, in «Rivista italiana di diritto del lavoro», 2016, n. 1, pp. 46 ss.; CGUE, Grande sezione, 20/12/2017, C-434/15, annotata da M. Delfino, *Il lavoro mediante piattaforme digitali tra tradizione e innovazione: il caso Uber*, in «Diritti lavori mercati», 2018, n. 2, pp. 337 ss.; nonché commissariamento di Uber Italy in relazione ad una indagine della Procura di Milano per caporalato, ai sensi dell'art. 603-*bis* c.p., cfr. Trib. Milano, sez. misure di prevenzione, del 27/5/2020, su cui V. Torre, *Destrutturazione del mercato del lavoro e frammentazione decisionale: i nodi problematici del diritto penale*, in «Questione Giustizia», 2020; A. Esposito, *I «riders» di Uber Italy s.r.l.*, in «Rivista italiana di diritto del lavoro», 2020, n. 2, pp. 558 ss.; A. Quattrocchi, *Le nuove manifestazioni della prevenzione patrimoniale: amministrazione giudiziaria e contrasto al «caporalato» nel caso Uber*, in «Giurisprudenza penale», 2020; A. Merlo, *Sfruttamento dei riders: amministrazione giudiziaria ad Uber per contrastare il «caporalato digitale»*, in «Sistema penale», 2020.

namento spazio-temporale della prestazione, permettendo di «staccarsi» dalla postazione di lavoro nei locali aziendali, creando l'illusione di maggiore libertà nella gestione del lavoro da svolgere; dall'altro consentono un controllo più penetrante e, dunque, rendono il lavoratore ancora più subordinato e isolato. In effetti, in tutti i casi in cui l'attività lavorativa «esce» totalmente o parzialmente dagli spazi aziendali e non si svolge più «nell'impresa», il potere direttivo e di controllo risultano sempre più intrecciati e richiedono quindi un ripensamento circa il loro contenuto e i loro limiti come tradizionalmente concepiti[7].

Si pensi a quegli algoritmi che stabiliscono schemi di turnazione, preselezionano il personale da assumere, verificano le assenze e le presenze in servizio mediante la scansione di dati biometrici, misurano la performance dei lavoratori (esigendo livelli quantitativi e qualitativi oggettivamente e istantaneamente misurati) e che permettono al datore di lavoro un controllo dell'attività dall'alto di una posizione di assoluto e pieno dominio informativo. È proprio l'elemento del dominio informativo che deve trovare un suo contrappeso in un nuovo assetto dei poteri sindacali come meglio si dirà più avanti.

La riflessione sull'utilizzo sempre più diffuso di macchine intelligenti e di algoritmi nei luoghi di lavoro deve pertanto spingere l'attuale dibattito in una prospettiva che investa ancora più fortemente la crisi di identità già in atto della stessa nozione di subordinazione[8], nata dal lavoro industriale nella fabbrica tradizionale.

[7] Per una riflessione su problematiche e spunti critici sull'applicazione dell'IA nell'organizzazione del lavoro, cfr. I. Piccinini e M. Isceri, *IA e datori di lavoro: verso una e-leadership?*, in «Lavoro Diritti Europa», 2021, n. 2.

[8] Sulla questione si segnalano: M. Magnani, *Subordinazione, eterorganizzazione e autonomia tra ambiguità normative e operazioni creative della dottrina*, in «Diritto delle Relazioni Industriali», 2020, pp. 105 ss.; A. Perulli, *Il diritto del lavoro «oltre la subordinazione»: le collaborazioni etero-organizzate e le tutele minime per i «riders» autonomi*, in «WP CSDLE "Massimo D'Antona".it», 2020, n. 410; Id., *Collaborazioni etero-organizzate, coordinate e continuative e subordinazione: come «orientarsi nel pensiero»*, in «Diritto delle Relazioni Industriali», 2020, n. 2, pp. 267 ss.; A. Maresca, *La disciplina del lavoro subordinato applicabile alle*

Coesistono infatti realtà nelle quali ci sono da una parte lavoratori – più o meno – autonomi che svolgono attività tradizionalmente proprie del lavoro subordinato e che, grazie alle nuove tecnologie oggi trovano più difficoltà a far ricondurre nell'alveo della subordinazione il loro lavoro in quanto il datore di lavoro è «smaterializzato» in un algoritmo; dall'altro i lavoratori subordinati che si trovano a rendere la loro prestazione da remoto, nelle forme del lavoro agile o del telelavoro (a volte anche in una forma snaturata rispetto a tali discipline, per ragioni di ordine pubblico sanitario), secondo un modello che sta diventando quello ordinario e generale di organizzazione del lavoro per milioni di lavoratori sia nel privato che nel pubblico.

Il risultato è quello di una smaterializzazione spazio-temporale dell'azienda che supera, o comunque, ridisegna le categorie tradizionali di subordinazione, conducendo sempre più la realtà lavorativa verso il concetto di eterorganizzazione[9], invece che di eterodirezione.

Proprio nel tentativo di ricercare delle soluzioni a tali problematiche, la Commissione europea con riferimento al fenomeno dei rider ha di recente[10] presentato una proposta di direttiva nella quale vengono dettate le regole per la tutela dei lavoratori delle piattaforme digitali. In particolare vengono definiti i parametri del livello di retribuzione, dell'orario di

collaborazioni etero-organizzate, in «Diritto delle Relazioni Industriali», 2020, n. 1, pp. 146 ss.; O. Razzolini, *I confini tra lavoro subordinato, etero-organizzato e lavoro autonomo coordinato: una rilettura*, in «Diritto delle Relazioni Industriali», 2020, n. 2, pp. 345 ss.; M.V. Ballestrero, *La dicotomia autonomia/subordinazione. Uno sguardo in prospettiva*, in «Labour & Law Issues», 6, 2020, n. 2, pp. 1 ss.; nonché, da ultimo, C. De Marco e A. Garilli, *L'enigma qualificatorio dei «riders». Un incontro ravvicinato tra dottrina e giurisprudenza*, in «WP CSDLE "Massimo D'Antona".it», 2021, n. 435, che così sintetizzano la questione: «L'organizzazione e la gestione dell'attività imprenditoriale si esplicano, dunque, per mezzo dei due strumenti tecnologici, piattaforma e algoritmo, la cui combinazione individua le modalità di esercizio dei poteri datoriali e quindi condiziona il processo di qualificazione dei rapporti di lavoro» (p. 6).

[9] Per uno studio approfondito del concetto di eterorganizzazione cfr. M. Pallini, *Il lavoro economicamente dipendente*, Padova, 2013.

[10] Proposta di direttiva della Commissione europea del 9/12/2021.

lavoro e del codice di abbigliamento e soprattutto i requisiti per il riconoscimento del diritto a essere inquadrati come dipendenti, con onere probatorio a carico del datore di lavoro che voglia dimostrarne invece i caratteri dell'autonomia.

Bruxelles ha inoltre affermato che il rispetto della privacy dei lavoratori da parte degli algoritmi che permettono il funzionamento delle piattaforme rientra tra gli obiettivi della proposta di direttiva sulle tutele ai lavoratori delle piattaforme digitali che fanno da intermediarie e organizzano il lavoro fornito da lavoratori anche autonomi a clienti terzi. La casistica riguarda sia il caso in cui la prestazione è effettuata in un luogo fisico specifico – come la consegna di cibo o il trasporto in auto – sia che avvenga online, ad esempio la codifica dei dati o i servizi di traduzione. In questo modello di business delle piattaforme di lavoro digitale, che si avvale quindi di tecnologie basate su algoritmi per abbinare in modo efficiente la domanda e l'offerta di lavoro o servizi, secondo la Commissione, mancano completamente le necessarie informazioni alle persone che vi lavorano su come funzionano gli algoritmi e su come vengono prese le decisioni che li riguardano.

La proposta di direttiva mira, quindi, innanzitutto a consentire alle persone che lavorano attraverso piattaforme digitali di avere il diritto di essere informate sui sistemi in uso di monitoraggio e decisionali automatizzati e su come gli stessi influenzano le loro condizioni di lavoro. Secondo la proposta di direttiva della Commissione europea anche i rappresentanti dei lavoratori e le autorità del lavoro dovranno avere accesso a tali informazioni, tale misura rappresenta infatti uno strumento fondamentale per un bilanciamento effettivo dei diritti in gioco.

Quanto alla protezione dei dati personali, le piattaforme di lavoro digitale non dovranno più essere in grado di raccogliere o elaborare dati personali che non siano direttamente correlati al lavoro svolto. Dovranno quindi essere programmate in modo tale che ciò non possa avvenire. Le piattaforme di lavoro digitali dovranno inoltre monitorare e valutare l'impatto delle decisioni individuali prese o supportate da sistemi decisionali e di monitoraggio automatizzati

sulle condizioni di lavoro, come la retribuzione o l'orario di lavoro.

Infine, le persone che lavorano sulla piattaforma avranno il diritto di ricevere spiegazioni sulle decisioni automatizzate che influiscono sulle loro condizioni di lavoro e di contestarle. Anche su tale particolare aspetto, il ruolo del sindacato con la previsione di apposite procedure, anche di conciliazione/arbitrato, potrà essere determinante per l'effettività delle tutele.

Le piattaforme di lavoro digitale – ha precisato la Commissione – dovranno garantire che le persone che svolgono lavori di piattaforma abbiano accesso a un contatto umano presso la piattaforma di lavoro digitale per discutere le decisioni che hanno un impatto significativo su di esse. Se il lavoratore chiede che sia rivista una decisione che lo riguarda, la piattaforma deve rispondere entro una settimana. Nel caso in cui la decisione violi i diritti della persona – ha concluso la Commissione – la piattaforma di lavoro digitale deve correggere la decisione o fornire un risarcimento.

Data la crescente diffusione nel processo produttivo dell'automazione e dell'IA e il loro sempre crescente utilizzo nell'ambito lavorativo si impone, dunque, una riflessione non solo sulle implicazioni e sugli effetti collaterali che ciò comporta in termini di nuovi rischi oltre che per la perdita dei diritti dei lavoratori, ma anche sulle possibili soluzioni. È proprio questo l'obiettivo che si è posta l'Unione europea.

Il lavoro svolto attraverso le piattaforme digitali comporta, altresì, anche significative conseguenze sul piano della sicurezza e della salute dei lavoratori, che andrebbero specificamente regolate. Il fenomeno in esame, aggiunge infatti, ai rischi diretti, relativi all'aumento degli infortuni, quelli indiretti da stress di lavoro correlato, dovuti ai ritmi di lavoro intensi, sollecitati in modo esponenziale dalla piattaforma e dal sistema di *rating* che costringe il lavoratore che vuole mantenere il proprio posto di lavoro ad anteporre tale interesse alla salvaguardia della propria salute psicofisica. Tali strumenti di lavoro, la cui installazione viene spesso invocata dai datori di lavoro proprio a tutela della sicurezza e della salute dei dipendenti nell'ambito della procedura di

cui all'art. 4 St. Lav., può essa stessa rappresentare invece un *vulnus* in tal senso.

È importante quindi che con riferimento allo specifico contesto lavorativo vengano attivate tutte le forme di tutela previste dal Testo Unico in materia di tutela della salute e della sicurezza nei luoghi di lavoro in relazione alla valutazione dei rischi correlati all'utilizzo di tali tecnologie, anche in base agli specifici algoritmi che il datore di lavoro decida di applicare agli strumenti di lavoro (ai sensi degli artt. 17, 28 e 29, d.lgs. 81/2008). Misure che sono applicabili a qualsiasi persona «indipendentemente dalla tipologia contrattuale» e quindi anche ai lavoratori non subordinati che – come definito dalla norma – operano «nell'ambito dell'organizzazione di un datore di lavoro pubblico o privato[11]».

Analoghe problematiche stanno emergendo, seppure più in sordina, con riferimento alla gestione degli appalti, dove in vari settori, anche impiegatizi quale quello bancario e assicurativo, il committente fornisce gratuitamente all'appaltatore un software o strumenti di lavoro quali videocamere o altri dispositivi di tracciamento indossabili, di cui devono necessariamente servirsi i dipendenti dell'appaltatore per rendere la prestazione.

Attraverso lo strumento di lavoro fornito dal committente, che impone processi tecnici e predeterminati di esecuzione della prestazione, il committente di fatto impartisce disposizione dettagliate e inderogabili sulla tempistica di svolgimento della prestazione, oltre a poter monitorare a distanza il corretto espletamento dell'attività lavorativa di ogni lavoratore assegnato all'appalto[12].

[11] Art. 2, d.lgs. 81/2008.

[12] L'amministrazione delle strade pubbliche norvegese aveva installato un sistema di videosorveglianza per monitorare la sicurezza nel cantiere di lavoro ed avere la possibilità di intervenire prontamente in caso di incidenti o infortuni ai dipendenti della società appaltatrice, ma in seguito, diversamente dalle finalità dichiarate originariamente, aveva invece utilizzato quelle telecamere e conservato le video registrazioni per verificare il regolare adempimento delle prestazioni degli appaltatori con l'obiettivo di contestarne l'operato e ottenere le prove per risolvere il contratto con la ditta Veidrift. Appurato che i trattamenti di dati personali tramite l'impianto di

Tali circostanze sollevano problematiche legate alla effettiva titolarità del rapporto di lavoro e alla possibile violazione delle norme di divieto di interposizione fittizia di mano d'opera. A ciò si aggiunge l'affievolimento delle tutele dei lavoratori eterodiretti in modo occulto dal committente, nei confronti del quale non trovano applicazione le tutele stabilite dall'art. 4 della l. 300/1970 sul divieto dei controlli a distanza (i cui oneri sono riferibili al solo diretto e formale datore di lavoro) e di conseguenza, nulla possono le organizzazioni sindacali operanti presso l'appaltatore, non avendo alcun diritto di informativa, né di interlocuzione con il committente.

Allo stesso modo, nessuna reale tutela per questi lavoratori può essere garantita dal Regolamento UE 2016/679 sulla tutela dei dati personali anche quando gli strumenti di lavoro o le apparecchiature di controllo a distanza sono installate e utilizzate dal datore di lavoro nei limiti indicati dall'art. 4, l. 300/1970, che al suo ultimo comma richiama il rispetto della normativa sul trattamento dei dati personali; tale statuizione non si applica infatti al committente che tratta i dati personali dei dipendenti dell'appaltatore sulla base di un suo interesse, tutto da verificare nella sua pretesa legittimità, al corretto adempimento dell'appalto e, quindi, al di fuori della base giuridica del contratto di lavoro e

videosorveglianza erano stati effettuati per scopi diversi da quelli dichiarati, e che neanche l'amministrazione delle strade pubbliche aveva cancellato le registrazioni video entro il termine di 7 giorni così come richiede la legge sui dati personali nazionale che nel 2018 ha implementato il GDPR nella legislazione norvegese, l'autorità per la protezione dei dati ha quindi inflitto alla Norwegian Public Roads Administration una multa di 400.000 corone norvegesi, corrispondenti a circa 37mila euro. Come precisa infatti l'autorità di controllo norvegese (Datatilsynet) nel provvedimento adottato lo scorso 25/8/2020 contro la Norwegian Public Roads Administration, l'uso di tali immagini per documentare le violazioni del contratto diversi mesi dopo che si sono verificati gli eventi è incompatibile con lo scopo originale, che era quello di attuare possibili misure di sicurezza immediate in caso di incidenti. Non era pertanto consentito utilizzare quelle registrazioni video per dare seguito ai rapporti contrattuali. Inoltre, tale utilizzo è risultato notevolmente svantaggioso per le parti contrattuali e i suoi dipendenti, essendo in conflitto con il modo in cui gli interessati possono aspettarsi che vengano utilizzati i loro dati personali.

dalle norme di legge che lo regolano e spesso senza neppure informare i lavoratori dell'appaltatore del trattamento che sta effettuando.

In tale contesto i lavoratori non sono effettivamente messi in grado di far valere i loro diritti, in quanto si trovano in situazione di soggezione non solo rispetto al proprio datore di lavoro, ma anche rispetto alla committenza, che potrebbe esercitare il diritto di non gradimento nei loro confronti.

Le organizzazioni sindacali che operano presso l'appaltatore oltre a non avere alcuna prerogativa nei confronti del committente, come già sottolineato, non hanno neppure alcun potere di rappresentanza diretta dei lavoratori nell'esercizio dei loro diritti di informativa e di accesso ai dati personali, a meno che non intervenga in tal senso il legislatore con un'integrazione normativa, come previsto dall'art. 80 del Regolamento UE 2016/679, di cui si dirà più avanti.

È quindi di fondamentale importanza che i dati dei lavoratori siano trattati solo a seguito di una preventiva e chiara informativa sulle finalità del trattamento e delle possibili conseguenze – e su una valida base giuridica che – in tale ambito non può di certo essere quella del consenso dell'interessato, perché il *metus* che contraddistingue tale rapporto non permette un consenso libero, come richiesto dal Regolamento UE 2016/679, oltre a non rendere effettivo l'esercizio del diritto di accesso dell'interessato, che dovrebbe quindi trovare in sede legislativa un suo rafforzamento.

2. *La Proposta di Regolamento su IA e la fine dell'opacità degli algoritmi*

Nel nuovo contesto di un rapporto di lavoro sempre più tecnologizzato assume una importanza decisiva l'intervento normativo europeo contenuto nella Proposta di Regolamento sull'intelligenza artificiale del 21/4/2021, che si pone lo scopo di incentivare lo sviluppo l'intelligenza artificiale nell'ambito di un approccio che punti alla sicurezza e all'affidabilità etica di tale tecnologia e nel contempo di garantire la tutela dei

principi fondamentali dell'Unione. Ciò in quanto l'interesse dichiarato dell'Unione è quello di preservare la leadership tecnologica dell'UE e assicurare che i cittadini europei possano beneficiare di nuove tecnologie sviluppate e operanti in conformità ai valori, ai diritti fondamentali e ai principi dell'Unione, con particolare riferimento al diritto alla non discriminazione, con requisiti specifici che mirano a ridurre al minimo il rischio di discriminazione algoritmica[13].

La detta Proposta di Regolamento sull'intelligenza artificiale risponde infatti ai principi dichiarati dalla Commissione e contenuti nel *Libro bianco sull'intelligenza artificiale* pubblicato il 19/2/2020, che definisce le opzioni strategiche su come conseguire il duplice obiettivo di promuovere l'adozione dell'IA minimizzando i rischi associati a determinati utilizzi di tale tecnologia. La Proposta di Regolamento sull'intelligenza artificiale ha quindi lo scopo dichiarato di attuare il secondo obiettivo espresso nel *Libro bianco*: quello di sviluppare un ecosistema di fiducia proponendo un quadro giuridico per un'IA affidabile. La proposta si basa sui valori e sui diritti fondamentali dell'UE e si prefigge di dare alle persone e agli utenti la fiducia per adottare le soluzioni basate sull'IA, incoraggiando al contempo le imprese a svilupparle.

Nella Proposta di Regolamento dell'intelligenza artificiale, altresì, si legge che tale normativa oltre a doversi sviluppare in coerenza con la Carta dei diritti fondamentali

[13] Sui rischi di discriminazione introdotti dalla rivoluzione digitale cfr. P. De Petris, *Le discriminazioni da algoritmo nella «gig economy»*, in «Argomenti di diritto del lavoro», 2020, n. 4, pp. 889 ss. Sempre in tema di discriminazione dell'algoritmo cfr. Tribunale di Bologna, ordinanza del 31/12/2020 (depositata il 2/1/2021), su ricorso *ex* art. 5, comma 2, del d.lgs. 216/2003 promosso da alcune OOSS che ha ritenuto discriminatorio per motivi sindacali l'algoritmo usato da Deliveroo per misurare il ranking reputazionale dei rider e, dunque, le condizioni di accesso alle sessioni di lavoro: il sistema di attribuzione dei punteggi di affidabilità e partecipazione penalizzava chi si assentava dal turno, non solo per futili motivi, ma anche in adesione ad uno sciopero o perché malato, pubblicata in A. Perulli, *La discriminazione algoritmica: brevi note introduttive a margine dell'Ordinanza del Tribunale di Bologna*, in «Lavoro Diritti Europa», 2021, n. 1.

dell'Unione europea deve essere coerente con il diritto derivato dell'Unione europea in vigore in materia di protezione dei dati personali (Regolamento UE 2016/679) e la direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie (direttiva UE 2016/680); che sono pertanto dalla stessa integrati con una serie di regole armonizzate applicabili alla progettazione, allo sviluppo e all'utilizzo di determinati sistemi di IA ad alto rischio, nonché di restrizioni concernenti determinati usi dei sistemi di identificazione biometrica remota.

Ci si augura che questa visione umanocentrica della regolamentazione dell'IA trovi concreta applicazione specialmente nell'ambito lavorativo, puntando al miglioramento delle condizioni di lavoro e non al suo esatto contrario. L'obiettivo deve, quindi, essere quello di ricercare delle soluzioni che garantiscano ai lavoratori l'effettivo esercizio dei propri diritti, compreso il diritto di opporsi alla profilazione, impedito di fatto dal particolare contesto di soggezione che contraddistingue il rapporto lavorativo.

E ciò potrà avvenire solamente se verrà riconosciuto il ruolo indispensabile di tutela collettiva dei diritti che possono svolgere in questo contesto i sindacati ai quali deve essere garantita la possibilità di richiedere e di conoscere le logiche applicate dagli algoritmi fin dalla loro ideazione e/o applicazione (*privacy by design*)[14] e di intervenire in caso di meccanismi decisionali opachi, per prevenire e evitare che l'IA o l'algoritmo applichino criteri basati su pregiudizi, creando discriminazioni e/o lesioni della salute dei lavoratori e, più in generale, dei diritti fondamentali.

La proposta di direttiva sull'IA dovrà quindi sicuramente integrare quanto già disposto dal Regolamento UE 2016/679 in tema di profilazione, che prevede specifici limiti in materia.

[14] In tal senso cfr. A. Donnini, *Profilazione reputazionale e tutela del lavoratore: la parola al Garante della Privacy*, in «Labour & Law Issues», 3, 2017, n. 1.

3. *Il divieto di profilazione nel Regolamento UE 2016/679*

L'intelligenza artificiale e gli algoritmi, in generale, realizzano un'attività di profilazione che è già regolata dal Regolamento generale sulla protezione dei dati personali.

Come è infatti noto l'art. 22 del Regolamento UE 2016/679, titolato *Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione* (C71, C72) stabilisce 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. Ciò in quanto la norma attribuisce il rango di diritto fondamentale a che le persone non siano sottoposte a decisioni automatizzate adottate usando dati personali trattati esclusivamente con mezzi automatici, senza l'intervento umano.

Tale processo decisionale automatizzato comprende la profilazione, che consiste in una forma di valutazione automatizzata degli aspetti personali concernenti una persona fisica; in particolare al fine di analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato (Considerando n. 71, art. 4, par. 4 e art. 22, Regolamento UE 2016/679).

La definizione di profilazione, secondo la tecnica legislativa europea, è contenuta infatti all'art. 4, par. 1, n. 4, dello stesso Regolamento UE 2016/679 e consiste in qualsiasi forma di trattamento automatizzato di dati personali per valutare determinati aspetti di 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 (C24, C30, C71-72).

Il Regolamento UE 2016/679 prevede dunque che gli interessati, nel nostro caso i lavoratori, non devono essere sottoposti a decisioni automatizzate che producono effetti

giuridici o comunque effetti significativi analoghi, qualora sia probabile che tali decisioni abbiano un impatto significativo sulle loro vite. Per tale ragione è necessaria una protezione specifica per evitare conseguenze negative.

Secondo il parere del Gruppo di lavoro articolo 29 (cd. WP29)[15], il diritto di non essere sottoposti a decisioni basate esclusivamente sul trattamento automatizzato di dati equivale a un divieto generale e non richiede che l'interessato debba attivamente opporsi a tale decisione[16].

Ai sensi del Regolamento UE 2016/679, infatti, il processo decisionale automatizzato che produce effetti giuridici o che incide significativamente sulle persone può essere ammissibile solo nei casi stabiliti dalla norma. Ovverosia se è necessario per la conclusione o l'esecuzione di un contratto di cui l'interessato è parte o se questo ha prestato il suo consenso esplicito o se è previsto per legge, e sempre che i diritti e le libertà e i legittimi interessi dell'interessato siano adeguatamente garantiti (art. 22, par. 2, Regolamento UE 2016/679).

In ogni caso, l'interessato deve essere sempre preventivamente informato sull'esistenza di un processo decisionale automatizzato che lo riguarda, compresa la profilazione. È suo diritto non solo sapere che il trattamento dei suoi dati avverrà con processi di profilazione, ma anche conoscere la logica utilizzata, le modalità di funzionamento dell'algoritmo e quali fattori l'algoritmo utilizza per calcolare i processi di valutazione (Convenzione n. 108 modernizzata, art. 9, par. 1, lett. *c* e punto 77), oltre che le conseguenze che possono derivare da tale trattamento. Inoltre, l'interessato ha il

[15] Il Gruppo articolo 29, in inglese *Working Party article 29* o WP29, è il Comitato europeo della protezione dei dati introdotto dal nuovo Regolamento europeo GDPR. Il gruppo articolo 29 è un organismo consultivo indipendente, «composto da un rappresentante delle varie autorità nazionali, dal Garante europeo della protezione dei dati, nonché da un rappresentante della Commissione».

[16] *Guidelines on Automated Individual Decision-Making and profiling for the purposes of Regulation* 2016/679, *Linee guida in materia di processi decisionali automatizzati e profilazione ai fini del regolamento UE* 2016/679, WP 251, 3/10/2017, p. 15.

diritto di accedere in ogni momento a tali informazioni che lo riguardano.

Le informazioni fornite agli interessati hanno lo scopo di assicurare la trasparenza del trattamento e consentire agli stessi di fornire consapevolmente il consenso o di ottenere l'intervento umano. Il titolare del trattamento è tenuto, in ogni caso, ad attuare misure appropriate per tutelare i diritti e le libertà degli interessati, tra i quali il diritto di ottenere l'intervento umano e la possibilità di esprimere la propria opinione e di contestare la decisione basata sul trattamento automatizzato dei propri dati personali.

L'obbligo per il titolare di prendere in considerazione il parere dell'interessato deriva dal diritto dello stesso di impugnare tali decisioni e di contestare eventuali inesattezze sui propri dati personali, nonché la pertinenza del profilo applicato (Convenzione n. 108 modernizzata, punto 75).

La raccomandazione del Consiglio d'Europa, CM/Rec (2010) 13 del Comitato dei ministri agli Stati membri sulla protezione delle persone con riguardo al trattamento automatizzato di dati personali nel contesto di attività di profilazione, sebbene non giuridicamente vincolante, specifica le condizioni per la raccolta dei dati nel contesto della profilazione, stabilendo disposizioni sulla necessità di garantire che il trattamento avvenga secondo equità, in modo legittimo, proporzionato e per finalità determinate e legittime. Contiene altresì disposizioni per garantire la qualità dei dati, prevedendo l'obbligo del titolare di adottare misure finalizzate a correggere fattori che comportano inesattezze, per minimizzare i rischi o gli errori che la profilazione può causare e l'obbligo di valutare periodicamente la qualità dei dati e degli algoritmi utilizzati.

Quanto fin qui richiamato riguarda l'attività di profilazione a prescindere dallo specifico contesto lavoristico, con riferimento al quale sono necessari i dovuti adeguamenti del caso, anche e soprattutto con riferimento alla base giuridica del consenso, che in tale ambito non può essere mai considerato liberamente rilasciato. È quindi indispensabile che la tutela dei diritti dei lavoratori sia effettivamente assicurata attraverso la possibilità di ricorrere all'intervento

sindacale, per evitare un'esposizione diretta dei lavoratori che potrebbero non esercitare i loro diritti per timore delle conseguenze.

Proprio a proposito di un processo di profilazione posto in essere dall'INPS, il Tribunale di Roma con una recente sentenza[17], ha confermato la decisione del Garante per la protezione dei dati personali con la quale l'INPS è stato sanzionato con una multa da € 40.000 per aver trattato i dati relativi alle assenze per malattia di 12,6 milioni di lavoratori pubblici e privati ai fini dell'attività di controllo medico-legale, oltre i limiti consentitegli dalla legge (che ne costituisce la base giuridica e quindi la legittimità del trattamento).

Ciò in quanto l'Istituto, al fine di indirizzare i controlli verso certificazioni meno «affidabili» e ottimizzare così i risultati dell'attività di controllo medico-legale, ha adottato processi di profilazione dei lavoratori tramite un software denominato «Data Mining/Savio». Tale programma attraverso degli algoritmi incrociava i dati relativi alla frequenza e alla durata delle malattie insieme ad altre variabili quali il numero delle precedenti inidoneità alle visite mediche di controllo, alla qualifica del lavoratore, al tipo di rapporto di lavoro, alla retribuzione, al settore e alla dimensione aziendale.

In tal modo, secondo il Garante per la protezione dei dati personali, l'INPS effettuava una vera e propria profilazione, sulla base di inferenze statistiche, realizzava prognosi comportamentali fondate su un calcolo probabilistico che, in quanto tali, sono sempre soggette a un margine di errore e per questo necessitano di garanzie adeguate per evitare false attribuzioni e valutazione erronee dei comportamenti individuali.

L'Istituto aveva proceduto, invece, a trattare i dati sensibili sulla malattia dei lavoratori senza una base giuridica, in quanto la legge non autorizzava tale tipo di analisi dei dati; senza informare i lavoratori del tipo automatizzato di trattamento; senza richiedere la verifica preliminare ai sensi dell'art. 17 del Codice in materia di protezione dei

[17] Tribunale di Roma, sentenza n. 4609/2020 del 3/3/2020.

dati personali e senza adottare alcuna misura a garanzia dei diritti dei lavoratori.

Il Garante per la protezione dei dati ha dunque stabilito con la propria decisione (provvedimento 29/11/2018, 9078812) che l'INPS per poter effettuare questo tipo di trattamento, consistente in una profilazione – tra l'altro – di dati sensibili, deve essere espressamente autorizzato da una legge che determini i limiti e le garanzie poste a tutela dei diritti degli interessati/lavoratori.

4. *La raccomandazione del Consiglio d'Europa del 1989 sul trattamento dei dati personali dei lavoratori*

Al fine, dunque, di inquadrare la corretta declinazione delle norme in materia di trattamento dei dati personali nel rapporto di lavoro, non si può prescindere da quanto previsto in ambito europeo sul trattamento dei dati personali in tale settore e di cui qui di seguito si offre un sintetico *excursus*.

A tale proposito la raccomandazione del Consiglio d'Europa sul trattamento dei dati in ambito lavorativo emanata nel 1989 e riveduta nell'aprile 2015 (Consiglio d'Europa, Comitato dei ministri [2015], raccomandazione Rec [2015] agli Stati membri sul trattamento dei dati personali nel contesto dell'occupazione) prevede che il trattamento dei dati personali nel settore del lavoro privato e pubblico deve sempre rispettare determinati principi e restrizioni, trai quali la consultazione dei rappresentanti dei dipendenti prima di introdurre sistemi di sorveglianza sul posto di lavoro. Viene inoltre stabilito che i datori di lavoro devono sempre preferire misure preventive, come ad esempio dei filtri, anziché controllare l'utilizzo di internet da parte dei dipendenti.

Un'indagine sui problemi più comuni relativi alla protezione dei dati nell'ambito lavorativo è reperibile nel documento del Gruppo di lavoro articolo 29 (Gruppo di lavoro articolo 29 [2017], parere sul trattamento dei dati sul posto di lavoro, WP 29, Bruxelles, 8/6/2017). Il Gruppo di lavoro articolo 29, con un altro documento (Gruppo di lavoro articolo 29 [2005], documento di lavoro sull'interpretazione

comune dell'articolo 26, paragrafo 1 della Direttiva 95/46/CE del 24/10/1995, WP 114, Bruxelles, 25/11/2005) ha inoltre analizzato l'importanza del consenso come base giuridica per il trattamento dei dati in ambito lavorativo, evidenziando come lo squilibrio economico tra il datore di lavoro che chiede il consenso e il lavoratore che lo presta solleva dubbi sul fatto che il consenso sia concesso liberamente.

Ai sensi della raccomandazione del Consiglio d'Europa, relativa alla protezione dei dati utilizzati per scopi di lavoro, i dati personali raccolti per scopi lavorativi dovrebbero essere ottenuti direttamente dal dipendente e, quindi, non da terzi. Per quanto riguarda poi i dati personali raccolti ai fini dell'assunzione, il loro trattamento deve essere limitato alle sole informazioni necessarie per valutare l'idoneità dei candidati e le loro prospettive di carriera.

La raccomandazione menziona specificamente anche i dati raccolti a fini di valutazione relativi alla produttività o al potenziale dei singoli dipendenti, stabilendo che i dati valutativi devono basarsi su giudizi equi e imparziali e non devono essere formulati in modo da risultare offensivi, nel rispetto dei principi di correttezza del trattamento e di esattezza dei dati personali. I lavoratori, inoltre, devono avere diritto di accedere ai propri dati e devono poter esercitare il diritto di rettifica e di cancellazione. In caso di trattamento di dati relativi a una valutazione, i lavoratori devono, pertanto, avere diritto di contestare tale valutazione. Tuttavia, questi diritti possono essere temporaneamente limitati nel caso di indagine interne. Se a un lavoratore sono negati l'accesso, la rettifica o la cancellazione di dati personali in ambito lavorativo, la legislazione deve prevedere procedimenti appropriati per contestare tale rifiuto.

Un aspetto specifico del diritto in materia di protezione dei dati personali nel rapporto di lavoro è considerato il ruolo dei rappresentanti dei lavoratori. Tali rappresentanti devono venire in possesso dei dati personali dei dipendenti nella misura in cui ciò sia necessario per consentire loro di rappresentare gli interessi dei lavoratori o se tali dati sono necessari per soddisfare o sorvegliare la conformità agli obblighi dei contratti collettivi.

I dati personali «sensibili» raccolti per scopi relativi al rapporto di lavoro possono essere trattati solo in casi particolari e nel rispetto delle garanzie stabilite dalla legislazione nazionale. I datori di lavoro possono chiedere ai dipendenti o ai candidati informazioni sul loro stato di salute e possono sottoporli a esame medico, soltanto se necessario per accertarne l'idoneità all'impiego, soddisfare esigenze di medicina, salvaguardare gli interessi vitali dell'interessato o di altri dipendenti e persone fisiche, consentire il riconoscimento delle prestazioni sociali o rispondere a richieste giudiziarie.

I dati relativi alla salute non possono essere raccolti da fonti diverse dal dipendente interessato, tranne quando sia stato acquisito il suo consenso esplicito e informato o quando lo preveda la normativa nazionale.

Il datore di lavoro può accedere alle comunicazioni elettroniche solo per motivi di sicurezza o per altri motivi legittimi, e tale accesso è consentito solo dopo che i dipendenti sono stati informati del fatto che il datore di lavoro può avere accesso a questo tipo di comunicazioni.

5. *Il parere del Gruppo di lavoro articolo 29 (WP 29) n. 2/2017 sul trattamento dei dati personali in ambito lavorativo*

Nel parere del Gruppo di lavoro articolo 29 (WP 29) n. 2/2017 sul trattamento dei dati personali in ambito lavorativo vengono esaminati una serie di scenari relativi al trattamento dei dati personali sul posto di lavoro in un contesto nel quale le nuove tecnologie e/o gli sviluppi di tecnologie esistenti hanno, o potrebbero presentare, potenziali elevati rischi per la vita privata dei dipendenti.

In tutti questi casi è onere dei datori di lavoro valutare se:

- l'attività di trattamento è necessaria e, in caso affermativo, quali sono i fondamenti giuridici che trovano applicazione;
- il trattamento proposto dei dati personali è corretto nei confronti dei dipendenti;

• l'attività di trattamento è proporzionata alle preoccupazioni sollevate;

• l'attività di trattamento è trasparente.

In particolare, il parere WP29 n. 2/2017 analizza i seguenti diversi scenari ricorrenti nell'ambito lavorativo.

5.1. *Trattamenti durante il processo di assunzione*

Erroneamente i datori di lavoro credono che sia legittimo poter esaminare i profili social dei potenziali candidati pubblicamente visibili a seconda delle impostazioni scelte dal titolare dell'account e altre informazioni pubblicamente disponibili nella rete durante il processo di assunzione. In realtà la pubblicità di tali informazioni non autorizza il datore di lavoro a trattare tali dati per proprie finalità semplicemente perché il profilo di una persona sui social media è pubblicamente accessibile.

Per poter procedere a un simile trattamento è necessario disporre di un fondamento giuridico, quale il consenso o, tutt'al più, un legittimo interesse del datore di lavoro a norma dell'articolo 6, lett. *f* Regolamento UE 2016/679, soltanto se tale esame è necessario ai fini del lavoro offerto; ad esempio per poter valutare rischi specifici correlati ai candidati che dovranno svolgere una funzione specifica e sempre che i candidati vengano informati correttamente in proposito (ad esempio nel testo dell'annuncio relativo al posto di lavoro).

In questo contesto, prima di esaminare il profilo del candidato sui social media, il datore di lavoro dovrebbe innanzitutto considerare se il profilo ha finalità commerciali o private, in quanto ciò può rappresentare un'indicazione importante dell'ammissibilità giuridica dell'esame di tali dati. Inoltre, il datore di lavoro è autorizzato a raccogliere e trattare i dati personali del candidato soltanto nella misura in cui tale raccolta è necessaria e pertinente per l'esecuzione del lavoro per il quale è stata presentata domanda. In linea di principio, i dati raccolti durante il processo di assunzione dovrebbero essere cancellati non appena sia evidente che non verrà fatta alcuna offerta di impiego o che l'offerta non sarà

accettata dal candidato. Il candidato deve, comunque, essere correttamente informato di qualsiasi trattamento dei suoi dati personali prima dell'avvio del processo di assunzione[18].

5.2. *Trattamenti derivanti da uno «screening» durante il periodo di impiego*

Attraverso i profili sui social media e lo sviluppo di nuove tecnologie di analisi, i datori di lavoro hanno (o possono ottenere) la capacità tecnica di effettuare uno *screening* permanente dei dipendenti, raccogliendo ad esempio informazioni riguardanti i loro amici, opinioni, credenze, interessi, spostamenti, atteggiamenti e comportamenti, acquisendo quindi dati che afferiscono anche alla vita privata e familiare.

È illegittimo lo *screening* durante il periodo di impiego dei profili dei dipendenti sui social media su una base generalizzata, nonché la richiesta del datore di lavoro di avere accesso alle informazioni condivise da un dipendente o da un candidato con altre persone sui social media. A titolo esemplificativo il WP29 nel proprio parere specifica che un datore di lavoro che monitora i profili LinkedIn di *ex* dipendenti per la durata dell'applicazione delle clausole di non concorrenza è legittimo se la finalità del monitoraggio è il controllo del rispetto di tali clausole, con riferimento ai soli *ex* dipendenti soggetti a tali clausole e fintantoché il datore di lavoro riesca a dimostrare che il monitoraggio è necessario per proteggere i propri legittimi interessi, sempre che non esistano altri mezzi meno invasivi e che gli *ex* dipendenti siano stati adeguatamente informati sulla por-

[18] Cfr. anche il documento del Consiglio d'Europa, *Raccomandazione CM/Rec(2015)5 del Comitato dei ministri agli Stati membri sul trattamento di dati personali nel contesto occupazionale*, paragrafo 13.2 (1/4/2015, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/export/4224268). Qualora il datore di lavoro desideri conservare tali dati in previsione di ulteriori opportunità lavorative, ne deve informare l'interessato, di conseguenza, il quale avrà la possibilità di opporsi a tale ulteriore trattamento; in quest'ultimo caso, i dati devono essere cancellati (*ibidem*).

tata del monitoraggio sistematico delle loro comunicazioni pubbliche. Solo in questo caso, il datore di lavoro potrà fare affidamento sul fondamento giuridico del cd. legittimo interesse, di cui all'articolo 6, lettera *f* del Regolamento UE, 2016/679.

Inoltre, secondo il parere del WP29 i dipendenti non devono essere tenuti a utilizzare un profilo sui social media messo a disposizione dal loro datore di lavoro, anche qualora ciò sia specificamente previsto in considerazione delle mansioni affidate (ad esempio, quella di agire da portavoce di un'organizzazione). I dipendenti devono conservare l'opzione di disporre di un profilo non pubblico, ossia «non lavorativo», che possono utilizzare in sostituzione del profilo «ufficiale» correlato al datore di lavoro, e ciò dovrebbe essere specificato nelle condizioni del contratto di lavoro.

5.3. *Trattamenti risultanti dal monitoraggio dell'uso delle tecnologie dell'informazione e della comunicazione sul posto di lavoro*

Il monitoraggio delle comunicazioni elettroniche sul posto di lavoro (ad esempio, telefono, navigazione in internet, posta elettronica, messaggistica istantanea, VOIP, ecc.) è stato tradizionalmente considerato la minaccia principale per la vita privata dei dipendenti. Nel *Documento di lavoro riguardante la vigilanza sulle comunicazioni elettroniche sul posto di lavoro* del 2001, il Gruppo di lavoro ha tratto una serie di conclusioni sul monitoraggio dell'utilizzo di posta elettronica e internet, che devono essere rilette alla luce degli sviluppi tecnologici che hanno consentito nuove modalità di monitoraggio potenzialmente più intrusive e pervasive quali:

– strumenti per la prevenzione della perdita di dati (DLP) che monitorano le comunicazioni in uscita per individuare eventuali violazioni dei dati;

– sistemi di firewall di nuova generazione (NGFW, *Next-Generation Firewall*) e di gestione unificata delle minacce (UTM, *Unified Threat Management*), che possono mettere a disposizione una varietà di tecnologie di monitoraggio,

tra cui quelle di *deep packet inspection* (ispezione profonda dei pacchetti), intercettazione TLS, filtraggio dei siti web, filtraggio dei contenuti, rendicontazione sulle applicazioni, informazioni relative all'identità degli utenti e (come descritto in precedenza) prevenzione della perdita di dati. Tali tecnologie possono essere altresì utilizzate individualmente, a seconda del datore di lavoro;

– applicazioni e misure atte a garantire la sicurezza che prevedono la registrazione dell'accesso dei dipendenti ai sistemi del datore di lavoro;

– la tecnologia *eDiscovery*, che si riferisce a qualsiasi processo in cui si effettuano ricerche di dati elettronici per utilizzarli come prova;

– il tracciamento dell'utilizzo di applicazioni e dispositivi tramite software invisibili, sia sul computer da tavolo che nel cloud;

– l'uso sul posto di lavoro di applicazioni per ufficio fornite come servizio cloud, le quali consentono in teoria di effettuare una registrazione molto dettagliata delle attività dei dipendenti;

– il monitoraggio di dispositivi personali (ad esempio computer, telefoni cellulari, tablet) che i dipendenti mettono a disposizione per lo svolgimento del loro lavoro in conformità con una specifica politica di utilizzo denominata *bring your own device* (BYOD, ossia utilizza i tuoi dispositivi privati), nonché il ricorso alla tecnologia *Mobile Device Management* (gestione dei dispositivi mobili) che consente la distribuzione di applicazioni, dati e impostazioni di configurazione, nonché patch per dispositivi mobili; e l'uso di dispositivi indossabili (ad esempio dispositivi per il fitness e la salute).

È possibile che un datore di lavoro implementi una soluzione di monitoraggio «omnicomprensiva», ad esempio un insieme di pacchetti per la sicurezza che gli consentano di monitorare l'utilizzo di tutte le tecnologie dell'informazione e della comunicazione sul posto di lavoro, rispetto al semplice monitoraggio di posta elettronica e/o siti web, come accadeva un tempo. Le conclusioni adottate nel documento WP29 si applicano a qualsiasi sistema che consente un tale monitoraggio.

A tale proposito il WP29 che esemplifica i principi sopra riportati ha precisato che nel caso in cui un datore di lavoro intenda utilizzare un apparecchio di intercettazione TLS per decrittare ed esaminare il traffico protetto al fine di individuare eventuali azioni dolose, possono sorgere problemi sulla liceità del trattamento di dati in quanto l'apparecchio è in grado di registrare e analizzare l'intera attività di un dipendente mentre è online sulla rete dell'organizzazione. In questo caso il legittimo interesse del datore di lavoro, costituito dalla necessità di proteggere la rete e i dati personali dei dipendenti e dei clienti dall'accesso non autorizzato o dalla perdita di dati, non giustifica un monitoraggio di tutte le attività online dei dipendenti e rappresenta una risposta sproporzionata e un'interferenza con il diritto alla segretezza delle comunicazioni. Il datore di lavoro dovrebbe quindi considerare altri mezzi, meno invasivi, per proteggere la riservatezza dei dati dei clienti e la sicurezza della rete.

Nella misura in cui un'intercettazione del traffico TLS possa qualificarsi come strettamente necessaria, l'apparecchio dovrebbe essere configurato in maniera tale da impedire la registrazione permanente dell'attività dei dipendenti, ad esempio bloccando il traffico sospetto in entrata o in uscita e reindirizzando l'utente a un portale informativo nel quale egli può chiedere un riesame di tale decisione automatizzata. Tuttavia, nel caso in cui una certa forma di registrazione generale dei dati si renda strettamente necessaria, l'apparecchio può essere configurato anche per non conservare i dati di registro, a meno che l'apparecchio non segnali il verificarsi di un incidente, riducendo così al minimo le informazioni raccolte.

Come buona prassi, il datore di lavoro potrebbe offrire un accesso alternativo non monitorato ai dipendenti, ad esempio offrendo un accesso wi-fi gratuito oppure mettendo a disposizione dispositivi o terminali indipendenti (dotati di opportune misure di salvaguardia per garantire la riservatezza delle comunicazioni), tramite i quali i dipendenti possano esercitare il loro legittimo diritto di utilizzare le strutture di lavoro per un determinato uso privato. Inoltre, i datori di lavoro dovrebbero valutare alcuni tipi di traffico la cui inter-

cettazione mette a repentaglio il giusto equilibrio tra i loro legittimi interessi e la vita privata, ad esempio l'uso di posta elettronica privata, visite a siti online di servizi bancari e siti web legati alla salute, onde configurare in maniera appropriata l'apparecchio in modo da non intercettare comunicazioni in circostanze non conformi al criterio di proporzionalità. È altresì necessario informare i dipendenti sul tipo di comunicazioni che l'apparecchio è inteso monitorare.

Si dovrebbe sviluppare e rendere facilmente e costantemente accessibile a tutti i dipendenti un regolamento relativo alle finalità per le quali i dati delle registrazioni sospette possono essere consultati e quali persone possono farlo, anche al fine di fornire una guida sull'uso accettabile e inaccettabile della rete e delle strutture.

Ciò consentirebbe ai dipendenti di adattare il proprio comportamento in maniera da evitare di essere monitorati quando utilizzano legittimamente le strutture di lavoro informatiche per uso privato. Come buona prassi, una tale politica dovrebbe essere riesaminata, almeno una volta l'anno, per valutare se la soluzione di monitoraggio scelta dia i risultati previsti e se esistono altri strumenti o mezzi meno invasivi per conseguire le medesime finalità.

Indipendentemente dalla tecnologia in questione o dalle sue capacità, la base giuridica del legittimo interesse di cui all'articolo 6, lettera *f*, è disponibile soltanto se il trattamento dei dati soddisfa determinate condizioni. Ovverosia, innanzitutto, i datori di lavoro che utilizzano questi prodotti e queste applicazioni devono valutare la proporzionalità delle misure che stanno attuando e se sia possibile adottare ulteriori azioni per attenuare o ridurre la portata e l'impatto del trattamento dei dati tramite una valutazione d'impatto sulla protezione dei dati prima di introdurre qualsiasi tecnologia di monitoraggio. In secondo luogo, i datori di lavoro devono attuare e comunicare politiche che descrivano l'utilizzo consentito della rete e delle attrezzature dell'organizzazione dettagliando con precisione il trattamento in atto.

Nel tentativo di dare concretezza ai principi richiamati, il WP29 specifica che nel caso in cui un datore di lavoro utilizzi uno strumento per la prevenzione della perdita di dati

con l'obiettivo di monitorare automaticamente i messaggi di posta elettronica in uscita al fine di impedire la trasmissione non autorizzata di dati proprietari (ad esempio dati personali del cliente), la necessità dello strumento di prevenzione della perdita di dati e il suo utilizzo possono essere pienamente giustificati solo se si realizza il giusto equilibrio tra i legittimi interessi del datore di lavoro e il diritto fondamentale alla protezione dei dati personali dei lavoratori[19].

Per poter far valere il proprio legittimo interesse, quindi, il datore di lavoro deve adottare misure che attenuino i rischi. Ad esempio, le regole seguite dal sistema per classificare un messaggio di posta elettronica come potenziale violazione di dati dovrebbero essere assolutamente trasparenti agli utenti e, laddove lo strumento classifichi un messaggio di posta elettronica in uscita come possibile violazione di dati, il mittente dovrebbe ricevere, prima della trasmissione del messaggio, un messaggio di avviso in modo da poter annullare la trasmissione[20].

[19] Cfr. anche *Copland contro Regno Unito* (2007) 45 EHRR 37, 25 BHRC 216, 2 ALR Int'l 785 (2007) ECHR 253 (http://www.bailii.org/eu/cases/ECHR/2007/253.html), nell'ambito del quale la Corte ha dichiarato che i messaggi di posta elettronica inviati dai locali aziendali e le informazioni desunte dal monitoraggio dell'uso di internet potrebbero costituire parte della corrispondenza e della vita privata di un dipendente e che la raccolta e la conservazione di tali informazioni senza che il dipendente ne sia a conoscenza costituirebbero un'interferenza con i diritti dei lavoratori, nonostante la Corte non si sia espressa in merito al fatto che tale monitoraggio non sarebbe assolutamente necessario in una società democratica.

[20] Cfr. *Halford contro Regno Unito* (1997) ECHR 32 (http://www.bailii.org/eu/cases/ECHR/1997/32.html), nel contesto del quale la Corte ha dichiarato che «le chiamate telefoniche provenienti da locali aziendali e da casa possono rientrare nelle nozioni di "vita privata"e "corrispondenza" ai sensi dell'articolo 8, paragrafo 1 [della Convenzione]»; e *Barbulescu contro Romania* (2016) ECHR 61 (http://www.bailii.org/eu/cases/ECHR/2016/61.html), riguardante l'uso di un account professionale di messaggistica istantanea per la corrispondenza personale, nel contesto del quale la Corte ha dichiarato che il monitoraggio dell'account da parte del datore di lavoro è stato limitato e proporzionato; nonostante il parere contrario del giudice Pinto de Albuquerque che ha sostenuto la necessità di realizzare un equilibrio attento.

Secondo il parere del WP29 in alcuni casi il monitoraggio dei dipendenti è possibile non tanto grazie a tecnologie specifiche, bensì semplicemente perché i dipendenti sono tenuti a utilizzare applicazioni online messe a disposizione dal datore di lavoro che elaborano dati personali.

Un esempio è l'uso di applicazioni per ufficio basate sul cloud (ad esempio editori di testo, calendari, applicativi di social networking). In tali casi è necessario che i datori di lavoro garantiscano che i dipendenti possano designare taluni spazi privati ai quali il datore di lavoro non può accedere, fatte salve circostanze eccezionali. È il caso, ad esempio, dei calendari, spesso utilizzati anche per appuntamenti privati. Qualora il dipendente classifichi un appuntamento come «privato» o annoti tale osservazione nei dettagli dell'appuntamento stesso, ai datori di lavoro (e agli altri dipendenti) non deve essere consentito esaminare il contenuto dell'appuntamento.

Talvolta, in questo contesto, il requisito della sussidiarietà implica che non sia possibile attuare alcun monitoraggio. È il caso, ad esempio, in cui l'uso proibito di servizi di comunicazione può essere impedito bloccando l'accesso a taluni siti web. Qualora sia possibile bloccare i siti web, anziché monitorare continuamente tutte le comunicazioni, occorre optare per il blocco, in maniera da rispettare il requisito di sussidiarietà. Più in generale, devono essere preferite le soluzioni tecniche atte a prevenire gli abusi, rispetto a quelle atte alla rilevazione degli stessi, a maggiore garanzia degli stessi interessi del datore di lavoro, e senza la necessità di spendere risorse per individuare eventuali usi impropri.

5.4. *Trattamenti risultanti dal monitoraggio dell'uso delle tecnologie dell'informazione e della comunicazione al di fuori del posto di lavoro*

L'utilizzo delle tecnologie dell'informazione e della comunicazione al di fuori del posto di lavoro è diventato più comune a seguito della crescita di politiche di lavoro a domicilio, lavoro a distanza e utilizzo dei propri dispositivi

personali (*bring your own device*). Le funzionalità offerte da tali tecnologie possono rappresentare un rischio per la vita privata dei dipendenti, in quanto spesso i sistemi di monitoraggio presenti sul posto di lavoro vengono estesi alla sfera domestica dei dipendenti nel momento in cui questi utilizzano tali apparecchiature.

5.5. *Il monitoraggio del lavoro a domicilio e del lavoro a distanza*

È sempre più comune per i datori di lavoro offrire ai dipendenti la possibilità di lavorare da remoto, ad esempio, da casa e/o in viaggio. In generale, la possibilità di lavorare da remoto implica che il datore di lavoro rilascia ai dipendenti apparecchiature TIC o software che, una volta installati a casa o sui dispositivi personali, consentono ai dipendenti di avere lo stesso livello di accesso alla rete, ai sistemi e alle risorse del datore di lavoro del quale beneficerebbero se fossero sul posto di lavoro, a seconda del grado di attuazione.

Sebbene possa essere uno sviluppo positivo, il lavoro a distanza presenta anche un rischio aggiuntivo per il datore di lavoro, in quanto i dipendenti che hanno accesso remoto all'infrastruttura aziendale non sono vincolati dalle misure fisiche di sicurezza che possono essere messe in atto presso i locali del datore di lavoro. Senza l'attuazione di adeguate misure tecniche, pertanto, il rischio di accesso non autorizzato aumenta e può provocare la perdita o la distruzione di informazioni, ivi inclusi i dati personali dei dipendenti o dei clienti.

Al fine di attenuare tale rischio, i datori di lavoro potrebbero pensare di essere giustificati a utilizzare pacchetti software (sia in modalità locale che nel cloud) in grado di registrare i tasti premuti e i movimenti compiuti dal mouse, di acquisire schermate visualizzate (in maniera casuale o a intervalli prestabiliti), di registrare le applicazioni utilizzate (e la durata del loro impiego) nonché, su dispositivi compatibili, di attivare telecamere web e raccogliere così filmati registrati. Tali tecnologie sono messe ampiamente a disposizione da terzi, tra i quali i prestatori di servizi cloud. Tuttavia, il trattamento

dei dati personali dei dipendenti che comporta l'adozione di tali tecnologie è sproporzionato ed è altamente improbabile che il datore di lavoro disponga di un fondamento giuridico e di un legittimo interesse per registrare tale tipologia di dati.

La corretta chiave sta nell'affrontare il rischio posto dal lavoro a domicilio o a distanza in maniera proporzionata e non lesiva di altri diritti, a maggior ragione poi nei casi in cui i confini tra l'uso aziendale e privato degli strumenti di lavoro sono labili.

5.6. *«Bring your own device» (BYOD)*

A causa dell'aumento della popolarità, delle caratteristiche e delle capacità dei dispositivi elettronici di consumo, i datori di lavoro possono trovarsi nella situazione di gestire le richieste di dipendenti che intendono utilizzare i loro dispositivi personali sul posto di lavoro per svolgere i propri compiti. Tale fenomeno è noto come *bring your own device* (abbreviato in BYOD), e indica appunto l'utilizzo di propri dispositivi personali.

L'attuazione efficace di questa politica può comportare una serie di vantaggi per i dipendenti, tuttavia, per definizione, il dispositivo del dipendente sarà in parte usato per fini personali, con più probabilità in determinati momenti della giornata (ad esempio la sera e nei fine settimana). Di conseguenza, esiste la possibilità concreta che l'uso di dispositivi propri da parte dei dipendenti comporti un trattamento, ad opera dei datori di lavoro, di informazioni non aziendali eventualmente riguardanti anche i loro familiari che utilizzino i dispositivi in questione.

Nei rapporti di lavoro, i rischi per la vita privata derivanti dall'uso di dispositivi propri sono comunemente associati a tecnologie di monitoraggio che raccolgono identificatori quali gli indirizzi MAC, oppure ai casi in cui il datore di lavoro accede al dispositivo del dipendente con la giustificazione di effettuare una scansione per finalità di sicurezza, ad esempio per rilevare la presenza di malware. In questi ultimi casi esistono numerose soluzioni commerciali che consentono

la scansione di dispositivi privati, tuttavia, il loro utilizzo potrebbe concedere potenzialmente l'accesso a tutti i dati presenti sul dispositivo, pertanto devono essere gestite con attenzione. In linea di principio, pertanto, non si dovrebbe accedere alle sezioni del dispositivo che si presume siano utilizzate esclusivamente per scopi privati (ad esempio, la cartella dedicata alla conservazione di immagini scattate tramite il dispositivo).

Il monitoraggio dell'ubicazione e del traffico di tali dispositivi può essere considerato rientrare nel legittimo interesse di proteggere i dati personali per i quali il datore di lavoro è responsabile in qualità di titolare del trattamento; tuttavia, potrebbe essere illecito quando riguarda un dispositivo personale di un dipendente e permette di acquisire anche dati relativi alla sua vita privata e familiare. Per impedire il monitoraggio delle informazioni private, è necessario che siano attuate misure appropriate per distinguere tra l'uso privato e quello aziendale del dispositivo.

I datori di lavoro dovrebbero, altresì, attuare sistemi che consentano il trasferimento sicuro, tra il dispositivo del dipendente e la propria rete, dei propri dati presenti sul dispositivo. Il dispositivo potrebbe quindi essere configurato in modo tale da indirizzare tutto il traffico attraverso una VPN in ritorno nella rete aziendale, in modo da offrire un certo livello di sicurezza. Tuttavia, laddove utilizzi una simile misura, il datore di lavoro dovrebbe tenere conto del fatto che il software installato per finalità di monitoraggio costituisce un rischio per la vita privata del dipendente quando questi usa il dispositivo per fini personali. Si potrebbero anche utilizzare soluzioni di protezione supplementare quali lo *sandboxing*, che prevede la conservazione dei dati in un'applicazione specifica.

Qualora non sia possibile impedire il monitoraggio dell'uso privato, ad esempio se il dispositivo in questione consente l'accesso remoto a dati personali per i quali il datore di lavoro è il titolare del trattamento, deve essere valutata la possibilità di vietare l'uso di tali dispositivi di lavoro per fini privati.

5.7. *Gestione dei dispositivi mobili («mobile device management»)*

La gestione dei dispositivi mobili consente ai datori di lavoro di localizzare i dispositivi a distanza, di installare configurazioni e/o applicazioni specifiche e di eliminare dati su richiesta, nonché di registrare o tracciare il dispositivo in tempo reale, anche quando non ne è stato segnalato il furto. Un datore di lavoro può gestire questa funzionalità autonomamente oppure dandone incarico a terzi (con nomina di responsabile del trattamento ai sensi dell'art. 28 Regolamento UE 2016/679).

Prima di impiegare una simile tecnologia, laddove essa sia nuova o comunque nuova per il titolare del trattamento, è necessario effettuare una valutazione d'impatto sulla protezione dei dati (ai sensi dell'art. 35 del Regolamento UE 2016/679). Se dalla valutazione emerge che la tecnologia di gestione dei dispositivi mobili è necessaria in specifiche circostanze, si dovrebbe in ogni caso effettuare una valutazione della conformità ai principi di proporzionalità e sussidiarietà del trattamento dei dati risultante.

I datori di lavoro devono assicurarsi che i dati raccolti nel contesto di tale capacità di localizzazione remota siano trattati per finalità specifiche e non costituiscano, o non possano costituire, parte di un programma più ampio di monitoraggio continuo dei dipendenti. Anche in caso di finalità specifiche, le caratteristiche di tracciamento dovrebbero essere minimizzate (ai sensi dell'art. 5, par. 1, lett. *c*, Regolamento UE 2016/679). I sistemi di tracciamento possono essere progettati per registrare i dati relativi all'ubicazione senza renderli conoscibili al datore di lavoro: in tal caso, i dati relativi all'ubicazione dovrebbero essere resi disponibili soltanto nelle circostanze in cui il dispositivo venga segnalato come rubato o perso.

In ogni caso, i dipendenti i cui dispositivi sono inseriti in tali servizi di gestione dei dispositivi mobili devono sempre essere pienamente informati sul tipo di tracciamento attuato e sulle sue conseguenze nei loro confronti.

5.8. *Dispositivi indossabili*

I datori di lavoro sempre più di frequente richiedono ai loro dipendenti di indossare dispositivi atti a tracciarne e monitorarne la salute oltre che l'attività all'interno, e talvolta anche all'esterno, del posto di lavoro. Tuttavia, un tale trattamento implica il trattamento di dati relativi alla salute ed è pertanto vietato a norma dell'articolo 8 della Direttiva sulla protezione dei dati (e oggi dell'art. 9, Regolamento UE 2016/679).

Dato l'impari rapporto tra datori di lavoro e dipendenti, dovuto alla dipendenza finanziaria dei secondi nei confronti dei primi, nonché data la natura sensibile dei dati relativi alla salute, è altamente improbabile che possa essere concesso un consenso esplicito legalmente valido al tracciamento o al monitoraggio di tali dati, in quanto i dipendenti non sono sostanzialmente «liberi» di rilasciare tale consenso.

Anche qualora il datore di lavoro si rivolga a un terzo per la raccolta dei dati relativi alla salute e il terzo gli fornisca poi soltanto informazioni aggregate sugli sviluppi generali in materia di salute, tale trattamento secondo il parere del WP29 è comunque illecito.

Inoltre, come descritto nel parere WP29 n. 5/2014 sulle tecniche di anonimizzazione[21], è tecnicamente molto difficile garantire una completa anonimizzazione di tali dati. Anche in un contesto con più di mille dipendenti, considerata la disponibilità di altri dati sui dipendenti, il datore di lavoro potrebbe comunque essere in grado di individuare i singoli dipendenti disponendo di particolari indicazioni in merito alla loro salute, quali l'ipertensione o l'obesità.

Nel parere del WP29 viene riportato a titolo esemplificativo il caso di un'organizzazione che offra dispositivi di monitoraggio della forma fisica ai propri dipendenti come regalo generalizzato. I dispositivi contano il numero di passi

[21] Gruppo di lavoro articolo 29, *Parere 5/2014 sulle tecniche di anonimizzazione*, WP 216 del 10/4/2014, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_it.pdf.

compiuti dai dipendenti, ne registrano il battito cardiaco e i modelli di sonno nel corso del tempo.

Tali dati devono essere accessibili esclusivamente ai dipendenti e non al datore di lavoro. Qualsiasi dato del dipendente (in qualità di interessato) trattato dal prestatore di servizi/del dispositivo (in qualità di titolare del trattamento) deve rimanere tra le dette due parti e non può essere comunicato al datore di lavoro.

5.9. *Trattamenti relativi al rilevamento degli orari e delle presenze*

Anche i sistemi che consentono ai datori di lavoro di controllare chi può entrare nei loro locali e/o in determinate aree all'interno degli stessi possono consentire il tracciamento delle attività dei dipendenti. Sebbene tali sistemi esistano da diversi anni, le nuove tecnologie di tracciamento degli orari e delle presenze dei dipendenti sono ora più diffuse e sofisticate, come quelle che elaborano dati biometrici o il tracciamento di dispositivi mobili.

Nonostante tali sistemi possano costituire una componente importante del controllo di un datore di lavoro, essi presentano anche il rischio di fornire un livello invasivo di conoscenza e controllo in merito alle attività del dipendente sul posto di lavoro.

Per tale ragione, secondo il parere del WP29 un datore di lavoro che dispone di una sala server nella quale sono conservati in formato digitale i dati sensibili per l'attività aziendale e i dati personali relativi ai dipendenti e ai clienti, al fine di rispettare gli obblighi legali che impongono di proteggere tali dati dall'accesso non autorizzato, può installare un sistema di controllo degli accessi che registra l'ingresso e l'uscita dei dipendenti che dispongono dell'opportuna autorizzazione per accedere a tale stanza. In caso di perdita di un componente dell'apparecchiatura oppure di accesso non autorizzato ai dati o loro perdita o furto, le registrazioni conservate dal datore di lavoro gli consentono di stabilire chi ha avuto accesso alla stanza. In tale caso il trattamento

può essere svolto in virtù di un legittimo interesse a norma dell'articolo 6, lettera *f*, considerato che il dato è necessario e non viola il diritto alla vita privata dei dipendenti, purché i dipendenti ne siano adeguatamente informati. Tuttavia, il monitoraggio continuo della frequenza e degli orari precisi di entrata e uscita dei dipendenti secondo il parere di WP29 non può essere giustificato se tali dati vengono utilizzati anche per altre finalità, quali ad esempio la valutazione del rendimento dei dipendenti.

5.10. *Monitoraggio video e videosorveglianza*

Il monitoraggio video e la videosorveglianza continuano a presentare problemi analoghi in materia di tutela della vita privata dei dipendenti rispetto a quelli riscontrati in passato: tali sistemi consentono di acquisire continuamente informazioni sul comportamento del lavoratore[22]. Le modifiche più rilevanti relative all'applicazione di questa tecnologia nei rapporti di lavoro sono la possibilità di accedere facilmente a distanza ai dati raccolti (ad esempio tramite uno smartphone), la riduzione delle dimensioni delle telecamere (associata a un aumento delle loro capacità, ad esempio in termini di alta definizione) e il trattamento che può essere effettuato dalle nuove soluzioni di analisi video.

Grazie alle funzionalità offerte dalle soluzioni di analisi video, il datore di lavoro ha la possibilità di controllare le espressioni facciali del lavoratore utilizzando mezzi automatizzati al fine di individuare deviazioni da modelli di movimento predefiniti (ad esempio nel contesto di una fabbrica) e molto altro ancora. Ciò sarebbe sproporzionato nei confronti dei diritti e delle libertà dei dipendenti e, di conseguenza, in linea di principio, illecito. È probabile inoltre

[22] Cfr. il caso citato in precedenza, *Köpke contro Germania*; va altresì osservato che in alcune giurisdizioni è stata riconosciuta come ammissibile l'installazione di sistemi quali quelli di televisione a circuito chiuso al fine di provare un comportamento illecito; cfr. il caso Bershka presso la Corte costituzionale di Spagna.

che tale trattamento comporti la profilazione ed, eventualmente, l'adozione di decisioni automatizzate. Pertanto, i datori di lavoro dovrebbero astenersi dall'uso di tecnologie di riconoscimento facciale. Vi possono essere alcune eccezioni a questa regola, tuttavia, secondo il parere del WP29, tali scenari non possono essere utilizzati per invocare una legittimazione generale dell'utilizzo di tale tecnologia[23].

5.11. *Trattamenti di geolocalizzazione di veicoli utilizzati dai dipendenti*

Le tecnologie che consentono ai datori di lavoro di monitorare i propri veicoli sono attualmente ampiamente adottate, in particolare, nel contesto di organizzazioni che svolgono attività di trasporto o che dispongono di flotte di veicoli.

Qualsiasi datore di lavoro che utilizzi dispositivi telematici a bordo di veicoli raccoglierà dati in merito al veicolo e al singolo dipendente che lo utilizza. Tali dati possono includere non solo la posizione del veicolo (e quindi del dipendente) raccolta dai sistemi di tracciamento di base GPS, ma anche molte altre informazioni, a seconda della tecnologia, compreso il comportamento di guida. Talune tecnologie possono altresì consentire un monitoraggio continuo, tanto del veicolo quanto del conducente (si pensi ad esempio ai registratori di dati relativi ad eventi). Un datore di lavoro potrebbe essere tenuto a installare tale tecnologia di monitoraggio a bordo dei veicoli per dimostrare la conformità ad altri obblighi legali, ad esempio per garantire la sicurezza dei dipendenti che guidano tali veicoli. Il datore di lavoro può anche avere un legittimo interesse a poter individuare i veicoli in qualsiasi momento.

Sebbene i datori di lavoro possano disporre di un legittimo interesse a raggiungere tali scopi, occorre innanzitutto

[23] Inoltre, ai sensi del Regolamento generale sulla protezione dei dati, il trattamento di dati biometrici per finalità di identificazione deve basarsi su un'eccezione tra quelle previste all'articolo 9, paragrafo 2.

valutare se il trattamento per dette finalità sia necessario e se l'effettiva attuazione sia conforme ai principi di proporzionalità e sussidiarietà. Qualora sia consentito l'uso privato di un veicolo professionale, la misura più importante che un datore di lavoro può adottare per garantire il rispetto di tali principi consiste nell'offrire un'opzione di esclusione: in linea di principio, il dipendente dovrebbe avere la possibilità di disattivare temporaneamente il tracciamento della posizione qualora circostanze particolari lo giustifichino, ad esempio nel caso in cui si rechi a una visita medica. In questo modo, il dipendente può, di propria iniziativa, proteggere determinati dati relativi all'ubicazione considerati privati. Il datore di lavoro deve garantire che i dati raccolti non vengano utilizzati per un ulteriore trattamento illegittimo, per finalità di tracciamento o valutazione dei dipendenti.

Il datore di lavoro deve altresì informare con chiarezza i dipendenti che a bordo del veicolo aziendale da loro guidato è stato installato un dispositivo di tracciamento e che i loro movimenti vengono registrati durante l'uso di detto veicolo (e che, a seconda della tecnologia in questione, potrà essere registrato anche il loro comportamento di guida). Preferibilmente tali informazioni dovrebbero essere esposte in maniera visibile a bordo di ogni vettura, nel campo visivo del conducente.

È possibile che i dipendenti utilizzino veicoli aziendali al di fuori degli orari di lavoro, ad esempio per uso personale, a seconda delle politiche specifiche. Data la sensibilità dei dati relativi all'ubicazione, è improbabile che vi sia una base giuridica per il monitoraggio delle posizioni dei veicoli dei lavoratori al di fuori dall'orario di lavoro concordato. Tuttavia, laddove sussista una tale necessità, si dovrebbe prendere in considerazione un'attuazione che sia proporzionata ai rischi. Ciò potrebbe significare che, per prevenire il furto dell'auto, la posizione della stessa non venga registrata al di fuori dell'orario di lavoro a meno che il veicolo non abbandoni una zona ben definita (regione o persino Paese). Inoltre, la posizione dovrebbe essere visualizzata soltanto in caso di emergenza: ossia il datore di lavoro dovrebbe poter

attivare la «visibilità» della posizione, accedendo ai dati già memorizzati dal sistema, soltanto nel momento in cui il veicolo lasci una regione predefinita. Come indicato nel parere 13/2011 sui servizi di geolocalizzazione su dispositivi mobili intelligenti:

I dispositivi di tracciamento dei veicoli non sono dispositivi di tracciamento del personale, bensì la loro funzione consiste nel rintracciare o monitorare l'ubicazione dei veicoli sui quali sono installati. I datori di lavoro non dovrebbero considerarli come strumenti per seguire o monitorare il comportamento o gli spostamenti di autisti o di altro personale, ad esempio inviando segnali d'allarme in relazione alla velocità del veicolo.

Inoltre, come indicato nel parere 5/2005 sull'uso di dati relativi all'ubicazione al fine di fornire servizi a valore aggiunto:

può essere giustificato quando è effettuato nell'ambito dei controlli sul trasporto di persone o cose ovvero al fine di migliorare la distribuzione delle risorse per i servizi in località remote (ad esempio, in rapporto alla pianificazione in tempo reale delle operazioni) o quando si persegue un obiettivo di sicurezza che è collegato al lavoratore stesso o ai beni o veicoli a lui affidati. Viceversa, il Gruppo ritiene che il trattamento dei dati sia eccessivo se i lavoratori sono liberi di organizzare i loro spostamenti come desiderano, o se il controllo della loro attività lavorativa costituisce la sola finalità di tale trattamento e tale controllo potrebbe essere realizzato con altri mezzi[24].

5.12. *Registratori di dati relativi a eventi*

I registratori di dati relativi a eventi forniscono al datore di lavoro la capacità tecnica di trattare una quantità notevole di dati personali in merito ai dipendenti che guidano veicoli

[24] Gruppo di lavoro articolo 29, *Parere 13/2011 sui servizi di geolocalizzazione su dispositivi mobili intelligenti*, WP 185 del 16/5/2011, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_it.pdf.

aziendali. Tali dispositivi vengono installati con frequenza sempre maggiore a bordo dei veicoli con l'obiettivo di effettuare registrazioni video, possibilmente inclusive di audio, in caso di incidente.

Questi sistemi sono in grado di effettuare le registrazioni in determinati momenti, come ad esempio, in risposta a frenate improvvise, improvvisi cambiamenti di direzione o incidenti, nel qual caso vengono conservati anche i momenti immediatamente precedenti l'incidente; tuttavia tali sistemi possono anche essere impostati per effettuare un monitoraggio continuo. Successivamente queste informazioni possono essere utilizzate per osservare e riesaminare il comportamento di guida di una persona allo scopo di migliorarlo. Inoltre, molti di questi sistemi includono una funzionalità GPS che consente il tracciamento della posizione del veicolo in tempo reale e la conservazione per finalità di ulteriore trattamento di altri dettagli relativi alla guida, come la velocità del veicolo.

Tali dispositivi sono diventati particolarmente diffusi tra le organizzazioni che svolgono attività di trasporto o che dispongono di flotte notevoli di veicoli. Tuttavia, l'impiego di registratori di dati relativi a eventi può essere considerato lecito soltanto se esiste una necessità effettiva di trattare i risultanti dati personali del dipendente per finalità legittime e tale trattamento è conforme ai principi di proporzionalità e sussidiarietà.

Il caso preso in considerazione nel parere del WP29 è quello di un'impresa di trasporti che abbia dotato tutti i propri veicoli di una videocamera all'interno dell'abitacolo che registra suoni e video. La finalità del trattamento di questi dati è il miglioramento delle capacità di guida dei dipendenti. Le telecamere sono configurate in maniera tale da conservare le registrazioni qualora si verifichino frenate improvvise o bruschi cambiamenti di direzione. L'impresa presume di disporre di un fondamento giuridico per il trattamento nel proprio legittimo interesse a norma dell'articolo 7, lett. *f*, della Direttiva, al fine di proteggere la sicurezza dei propri dipendenti e quella degli altri conducenti.

Tuttavia, il legittimo interesse dell'impresa a monitorare i conducenti non prevale sui diritti di questi ultimi alla protezione dei loro dati personali. Il monitoraggio continuo dei dipendenti per mezzo di tali telecamere costituisce un'interferenza grave nel loro diritto alla tutela della vita privata. Esistono altri metodi, quali l'installazione di apparecchiature che impediscono l'utilizzo di telefoni cellulari, e altri sistemi di sicurezza, tra i quali un sistema avanzato di frenatura di emergenza o un sistema di avviso di deviazione dalla corsia, che possono essere impiegati per prevenire incidenti stradali e che possono essere più appropriati. Inoltre, esiste un'elevata probabilità che la presenza di tale registrazione determini il trattamento di dati personali di terzi (come i pedoni) e, per tale trattamento, il legittimo interesse dell'impresa non costituisca una giustificazione sufficiente.

5.13. *Trattamenti che implicano la divulgazione di dati dei dipendenti a terzi*

È diventata sempre più comune la prassi delle imprese di trasmettere i dati dei propri dipendenti ai propri clienti con l'obiettivo di garantire la prestazione di un servizio affidabile. In alcuni casi possono essere forniti anche dati non pertinenti ed eccessivi, a seconda della portata dei servizi forniti (come nel caso in cui si includa una foto di un dipendente). Tuttavia, in considerazione dello squilibrio di potere, i dipendenti non sono in una posizione tale da poter concedere un libero consenso al trattamento dei loro dati personali da parte del loro datore di lavoro, e se il trattamento dei dati non è proporzionale, il datore di lavoro non può fare valere alcun fondamento giuridico.

Nel caso in cui, pertanto, un'impresa di spedizioni invii ai propri clienti un messaggio di posta elettronica con un collegamento al nome e alla posizione dell'incaricato alla consegna della loro spedizione (dipendente di detta impresa) e l'impresa voglia altresì includere una foto in formato fototessera dell'incaricato alla consegna, ritenendo di poter fare valere quale fondamento giuridico per tale trattamento

il suo legittimo interesse (articolo 6, lett. *f*, Regolamento UE 2016/679) di consentire al cliente di verificare che la persona che effettua la consegna sia effettivamente la persona all'uopo preposta, in realtà non essendo necessario fornire ai clienti il nome e la foto dell'incaricato alla consegna, non sussiste alcun motivo di legittimazione per tale trattamento e, pertanto, l'impresa di spedizioni non è autorizzata a fornire tali dati personali ai clienti.

6. *L'indispensabile ruolo di bilanciamento e garanzia del sindacato*

Nel contesto di una nuova organizzazione del lavoro basata sulla IA e sull'utilizzo di algoritmi sarà necessario garantire una effettiva tutela dei diritti dei lavoratori finalizzata a creare quel clima di fiducia che permetta lo sviluppo sempre maggiore di tali tecnologie.

Ciò sarà possibile solo se verranno riconosciute nuove specifiche prerogative ai sindacati che prevedono la possibilità di contrattare e garantire una regolamentazione negoziale delle nuove tipologie di lavoro mediante piattaforma digitale o da remoto, le modalità di prestazione da remoto, nonché l'utilizzo dell'algoritmo, ma anche l'introduzione di misure di welfare aziendale di formazione e aggiornamento e soluzioni atte a prevenire rischi per la salute e la sicurezza dei lavoratori[25].

Per poter infatti prevenire e limitare gli effetti collaterali dei sistemi di IA che in sede valutativa e decisionale potrebbero derivare da difetti nella progettazione (o nei frequenti aggiornamenti del software o che si basano sull'apprendimento automatico) oppure dall'uso di dati e dai collegamenti tra di essi, in occasione del controllo sull'attività lavorativa o in sede preassunzionale, le organizzazioni sindacali devono essere messe in grado di poter conoscere e

[25] Così come d'altronde ha riconosciuto la Commissione europea nel *Libro bianco* del 2020 *Il coinvolgimento delle parti sociali sarà un fattore cruciale per garantire un approccio antropocentrico all'IA sul lavoro*.

valutare i criteri e le logiche utilizzate dagli algoritmi, anche in sede di progettazione e prima installazione di tali sistemi (*privacy by design*) e di poterne contestare l'illegittimità e la discriminatorietà, anche a posteriori.

Nonostante, infatti, la diffusa convinzione di crisma di scientificità ed «autorità» della valutazione algoritmica che appare più efficiente, oggettiva e affidabile del ragionamento umano, in realtà, si tratta di un processo che non è di certo immune da errori e pregiudizi i cui criteri devono poter essere conosciuti e valutati da chi vi è sottoposto e dalle autorità.

Per fare ciò è necessario, dunque, che le organizzazioni sindacali possano esercitare un proprio diritto originario di informativa e di partecipare al necessario intervento umano del processo automatizzato decisionale prima che il risultato del sistema di IA diventi definitivo, nonché di poter assistere il lavoratore in sede di contestazione degli esiti.

La partecipazione delle organizzazioni sindacali a tali processi, impensabile per il singolo lavoratore, è necessaria anche per combattere la speciosa neutralità e oggettività dell'algoritmo, che lungi dall'essere veramente imparziale, altro non è che la trasposizione tecnico-pratica di precise scelte e convinzioni umane, basate su assunti indimostrati[26].

Ma al di là di nuovi scenari della contrattazione collettiva (invero lontani dall'essere attuati) appare necessario un intervento normativo che permetta alle organizzazioni sindacali di proteggere i diritti dei lavoratori anche al di fuori dei casi in cui è applicabile l'art. 4, l. 300/1970, quindi, non solo nei confronti del diretto datore di lavoro, ma anche – come già

[26] In quest'ottica, è condivisibile l'invito contenuto nella recente Risoluzione del Parlamento UE di cui si è detto a «garantire che le relazioni industriali tra le piattaforme e i lavoratori siano adeguate alle nuove realtà di una società e un'economia digitalizzate e che siano chiarite includendo tali lavoratori nelle leggi vigenti in materia di lavoro e nelle disposizioni in materia di sicurezza sociale, al fine di migliorarne le condizioni di lavoro, le competenze e la formazione e di garantire loro orari di lavoro prevedibili», garantendo che «i lavoratori delle piattaforme possano costituire rappresentanze dei lavoratori e formare sindacati per concludere contratti collettivi».

sottolineato – nel caso in cui sia il committente a trattare i dati dei dipendenti dell'appaltatore.

Per fare ciò, il sindacato dovrebbe essere messo in grado di esercitare il proprio ruolo di tutela collettiva dei lavoratori alla protezione dei loro dati personali. A tale scopo non appare sufficiente la possibilità riconosciuta al singolo lavoratore di delegare l'organizzazione sindacale nell'esercizio dei suoi diritti, ai sensi dell'art. 80, par. 1, del Regolamento UE 2016/679; perché tale eventualità costringe i lavoratori a esporsi in prima persona, con il rischio di perdere il lavoro o l'assegnazione all'appalto, anche solo per conoscere l'esistenza di un trattamento dei loro dati.

Per rendere quindi effettiva la tutela dei dati personali e della conoscibilità dei criteri posti alla base del funzionamento dell'algoritmo nell'ambito lavorativo, anche al di là del contratto di lavoro (per le ragioni che si sono evidenziate), si auspica che il legislatore voglia cogliere l'opportunità offerta dal par. 2 dell'art. 80, Regolamento UE 2016/679, prevedendo la possibilità che il sindacato autonomamente, indipendentemente dal mandato conferito dall'interessato, abbia la facoltà di proporre reclamo all'autorità di controllo o giudiziale qualora ritenga che i diritti dei lavoratori/interessati siano stati violati.