



LaBoUR & Law Issues
Rights | Identity | Rules | Equality

**Sistemi di IA ad alto rischio e ruolo del sindacato
alla prova del *risk-based approach***

LOREDANA ZAPPALÀ
Università di Catania

vol. 10, no. 1, 2024

ISSN: 2421-2695



Sistemi di IA ad alto rischio e ruolo del sindacato alla prova del *risk-based approach*

LOREDANA ZAPPALÀ

Università di Catania

Associata di Diritto del lavoro

lzappala@lex.unict.it

ABSTRACT

The aim of the present study is to analyse the impact of the regulation of new technologies inspired by the risk-based approach, and in particular to examine the role of trade unions in the identification, assessment, management and mitigation of risks to workers' rights. Through the analysis of the regulation inspired by the risk-based approach (GDPR, IA Act and the proposal for a directive on the improvement of working conditions in platform work), the essay identifies a new trend towards the proceduralisation of risk management, functional to preserve the effectiveness and efficacy of traditional labour regulation.

Keywords: artificial intelligence; risk; digital work; accountability.

<https://doi.org/10.6092/issn.2421-2695/19875>

Sistemi di IA ad alto rischio e ruolo del sindacato alla prova del *risk-based approach*

SOMMARIO: 1. Digitalizzazione e approccio regolativo basato sul rischio. – 2. Diritto del lavoro e *governance* del rischio: una sfida accettabile? – 3. Le diverse declinazioni del *risk-based approach*: nel GDPR (la prospettiva *bottom-up*). – 3.1. (segue): nel IA Act (la prospettiva *top-down*). – 3.2. (segue): nella direttiva sul lavoro tramite piattaforme digitali (la prospettiva *command and control* collaborativa). – 4. *Rights-based* versus *risk-based approach*: quale ruolo per il sindacato? – 5. Il possibile contributo “a monte” del sindacato nella valutazione *risk-based*: a) del trattamento automatizzato (e non) dei dati. – 5.1. (segue): b) nei casi di utilizzo di sistemi di intelligenza artificiale ad alto rischio. – 5.2. (segue): c) nella valutazione di impatto sui sistemi automatizzati utilizzati dalle piattaforme di lavoro. – 6. La trasparenza come veicolo di emersione dei rischi per i diritti. – 7. Verso una co-progettazione della gestione del rischio.

1. Digitalizzazione e approccio regolativo basato sul rischio

Che il diritto nasca dall'esigenza di rendere prevedibile il futuro, dalla necessità di mettere ordine, di calcolare i rischi e di fare affidamento sui comportamenti altrui è storia nota. Così come, oggi, è storia nota la difficoltà del diritto di governare e regolare le tecnologie⁽¹⁾ e i dati, il loro utilizzo, i loro effetti e le conseguenti responsabilità.

La sfida normativa della società algoritmica e dei nuovi ambienti digitalizzati si scontra con problemi di vasta portata connessi alla dimensione globale e alla smaterializzazione dei luoghi ove le tecnologie operano, alla opacità e pervasività delle modalità computazionali e di controllo di dati, preferenze, azioni e in ultima analisi di intere vite di una moltitudine di persone, alla velocità e imprevedibilità delle innovazioni che rendono impossibile una regolazione realmente idonea a disciplinare il futuro.

Nel diritto dell'era della digitalizzazione concetti come la fattispecie, la calcolabilità, l'affidamento, e complessivamente le tecniche di regolazione *command and control*, sembrano recedere di fronte a un diverso approccio regolativo che, progressivamente, in questa materia, sposta il *focus* della regolazione sul rischio⁽²⁾, sulla sua previsione e gestione, e dunque su tecniche anche molto diversificate di

(1) S. Borelli -V. Brino - C. Faleri - L. Lazzeroni - L. Tebano - L. Zappalà, *Lavoro e tecnologie*, Giappichelli, 2020.

(2) Nell'ambito della dottrina lavoristica v. M. Barbera, “La nave deve navigare”. *Rischio e responsabilità al tempo dell'impresa digitale*, *q. Riv.*, 2023, n. 2, 3 ss.; P. Loi, *Il rischio proporzionato nella proposta di regolamento sull'IA e i suoi effetti nel rapporto di lavoro*, *federalismi.it*, 2023, n. 4, 239 ss.; M. Peruzzi, *Intelligenza artificiale e lavoro*, Giappichelli, 2023, 37 ss.; A. Aloisi - V. De Stefano, *Between risk mitigation and labour rights enforcement: Assessing the transatlantic race to govern AI-driven decision-making through a comparative lens*, *ELLJ*, 2023, n. 2, 283 ss.; per una più ampia analisi del rischio nel rapporto di lavoro P. Loi, *Rischio e sicurezza nel rapporto di lavoro*, *RGL*, 2013, n.3, 569 ss.

proceduralizzazione volte a evidenziare i rischi, a bilanciarne gli effetti e a mitigarne i pericoli; soprattutto se a essere messi a rischio sono i diritti e le libertà fondamentali dell'individuo. È indubbio, in effetti, che i sistemi e gli ambienti digitalizzati pur portando grandi vantaggi per la società, abbiano anche dato vita a sistemi e reti di comunicazione, di controllo e di sorveglianza collettiva e quotidiana senza precedenti che, spesso sotto le mentite spoglie di una razionalizzazione/oggettivizzazione della realtà, amplificano i rischi⁽³⁾ per le persone, la libertà, la dignità, la *privacy*, e così via lungo il catalogo dei diritti e delle libertà fondamentali dell'individuo.

Il processo di “rischificazione”⁽⁴⁾ della regolazione europea è, già da tempo, oggetto di numerose analisi che hanno evidenziato come l'approccio *risk-based* abbia iniziato a riguardare diversi aspetti connessi ai rischi per l'ambiente e per la salute e sicurezza, per poi – a partire dalla strategia per il mercato unico digitale⁽⁵⁾ – focalizzarsi sulle politiche digitali in materia di dati, servizi digitali, intelligenza artificiale, piattaforme, ecc. Si tratta di un processo anche fortemente contestato nella sua valenza, in quanto accusato di basarsi sulla sostituzione del principio di legalità formale che attribuisce diritti individuali con un modello di “autoregolamentazione per la gestione dell'innovazione in scenari incerti”⁽⁶⁾, ipoteticamente collaborativi, ma potenzialmente privi della capacità di una regolazione effettiva a tutela dei diritti.

Il modello di regolazione *risk-based* eleva il rischio a una sorta di *grundnorm*⁽⁷⁾ che, in modo flessibile e adattabile ai diversi contesti, offre un metodo per promuovere la “conformità” a principi generali in settori altamente tecnici in cui la regolamentazione completamente prescrittiva non appare in grado di tenere il passo con i nuovi sviluppi⁽⁸⁾. Secondo il *risk-based approach*, dunque, il rischio funge da parametro per l'interpretazione, la calibrazione e l'applicazione delle norme giuridiche, superando il tradizionale approccio regolativo *command and control*. Il funzionamento del modello e la sua concreta implementazione dipende dal contesto in cui viene applicato e prevede almeno due fasi principali. La prima fase, della valutazione, è dedicata alla previsione della probabilità e della gravità di un determinato evento, mentre la seconda fase, della gestione, prevede l'individuazione e l'implementazione di attività di controllo, mitigazione e correzione

⁽³⁾Sulle plurime dimensioni del rischio della società digitale v. D. Lupton, *Digital risk society*, in A. Burgess - A. Alemanno - J. Zinn (a cura di), *Routledge Handbook of Risk Studies*, London, 2016, 301 ss. Fondamentale è il rinvio a U. Beck, *Risk Society: Towards a New Modernity*, Sage, 1992.

⁽⁴⁾M. Macenaite, *The “Riskification” of European Data Protection Law through a two-fold Shift*, *European Journal of Risk Regulation*, 2017, n. 3, 506 ss.; M. Catanzariti, *Rischio e vulnerabilità nel modello europeo di intelligenza artificiale*, *SocietàMutamentoPolitica*, 2022, n. 13, 73 ss.

⁽⁵⁾COM(2010) 245 def., del 19 maggio 2010, Un'agenda digitale europea; COM(2015) 192 def., del 6 maggio 2015, Strategia per il mercato unico digitale in Europa.

⁽⁶⁾A. Aloisi - V. De Stefano, *Between risk mitigation and labour rights enforcement*, cit., 283 ss.

⁽⁷⁾A. Alemanno, *Regulating the European Risk Society*, in A. Alemanno - F. Den Butter - A. Nijssen - J. Torriti (a cura di), *Better Business Regulation in a Risk Society*, Springer, 2012, 37 ss.

⁽⁸⁾T. Mahler, *Between Risk Management and Proportionality: The Risk-based Approach in the EU's Artificial Intelligence Act Proposal*, *Nordic Yearbook of Law and Informatics*, 2021, 258 ss.

volte a ridurre il rischio fino a una soglia, individuabile secondo un *test* di proporzionalità, considerata come economicamente e/o (a secondo del contesto applicativo) socialmente tollerabile⁽⁹⁾.

A fronte di un modello regolativo evidentemente magmatico e procedurale, come quello che caratterizza il *risk-based approach*, è evidente come la lettura e l'interpretazione dei più recenti strumenti regolativi della società algoritmica non possano prescindere da un solido aggancio ai diritti fondamentali e alla prospettiva di una tecnologia affidabile, antropocentrica, che mette al centro le persone e che, appunto, rispetta i loro diritti fondamentali e le loro libertà.

Solo avendo chiara e tendendo ferma la descritta bussola interpretativa pare possibile analizzare la più recente regolazione delle nuove tecnologie, ispirata a un modello di *governance* del rischio, sulla quale occorre inevitabilmente confrontarsi, nella consapevolezza che tale nuova regolazione si affianca alla pure esistente e solida regolazione tradizionale che garantisce diritti e tutele, assicurandone l'effettività. Occorre approcciarsi a tale prospettiva nella consapevolezza di dover procedere a un bilanciamento di interessi, ma con la bussola ben salda e orientata sui diritti fondamentali riconosciuti e sulla necessità del loro rispetto, nella prospettiva di quello che è stato definito il nuovo costituzionalismo digitale europeo⁽¹⁰⁾: secondo il quale, attraverso l'impiego di un approccio basato sul rischio, si è cercato un temperamento tra la prospettiva "economica", ovvero la costruzione di un Mercato Unico Digitale economicamente sostenibile, e quella "costituzionale", che presuppone un approccio umanocentrico alle politiche digitali, rispettoso dei diritti fondamentali individuali e dei valori democratici.

2. Diritto del lavoro e *governance* del rischio: una sfida accettabile?

Elemento distintivo del modello *risk-based* è, come accennato, la sua funzione volta alla gestione e alla mitigazione del rischio, provando (con tecniche diversificate) a delineare soglie di "mitigazione" del rischio, di sua "tollerabilità" o di "inaccettabilità" dello stesso. Un approccio, dunque, che apparentemente stride con l'idea di un primato dei diritti fondamentali *tout court*, e di un diritto del lavoro pensato come tutto "fondamentale"⁽¹¹⁾, che nel tempo ha pesantemente sofferto la "valanga" della derogabilità, ma rispetto al quale il bilanciamento è stato effettuato sempre e prima di tutto su un piano valoriale, mettendo al centro della logica discorsiva l'intoccabilità di valori primari come la dignità della persona. Un approccio che, pertanto, sottopone a

⁽⁹⁾ R. Gellert, *The Risk-Based Approach to Data Protection*, Oxford, 2020.

⁽¹⁰⁾ G. De Gregorio, *The rise of digital constitutionalism in the European Union*, *International Journal of Constitutional Law*, 2021, n. 1, 41 ss.

⁽¹¹⁾ R. Del Punta, *I diritti fondamentali e la trasformazione del diritto del lavoro*, WP CSDLLE "Massimo D'Antona".IT – 333/2017.

forte tensione il diritto del lavoro che – seppure nato come un meccanismo di redistribuzione dei rischi di mercato e dei rischi sociali – si è sviluppato nella prospettiva costituzionalistica ispirata all’esigenza di assicurare un riequilibrio della posizione dei contraenti e sulla necessità di attribuire i rischi sul soggetto economicamente più forte. Se, “nel diritto del lavoro, tradizionalmente la distribuzione del rischio sociale viene regolata senza possibilità di graduazioni anzitutto attraverso la scelta del tipo contrattuale, restando poi aperta l’opzione tra il modello regolativo della norma sostanziale e quello della norma procedurale ove non si tratti di diritti considerati indisponibili e protetti da norme inderogabili”⁽¹²⁾, nel nuovo approccio *risk-based*, il rischio non solo è insito nella realtà, ma nemmeno è sempre eliminabile dalla regolazione, che tutt’al più prevede – se il rischio è alto – meccanismi di mitigazione per renderlo “tollerabile”. Come è stato rilevato, tale approccio incide profondamente anche sul regime di responsabilità degli operatori, in quanto sposta una parte della responsabilità dall’aver causato un danno, al non aver adottato – in un’ottica di *compliance* – tutte le misure necessarie per averlo previsto, prevenuto e contenuto. È indubitabile che il *risk-based approach*, a differenza del principio di precauzione⁽¹³⁾, accetta il rischio; ma forse è anche vero che a differenza di altri tipi di rischio, quali quelli in materia di salute e sicurezza negli ambienti di lavoro, i rischi della società algoritmica non siano ancora nemmeno del tutto immaginabili e aprioristicamente ponderabili e, dunque, *ex ante* catalogabili come rischi assolutamente non tollerabili come quelli alla vita o alla salute.

Probabilmente, al fine di valutare e verificare gli esiti regolativi dell’approccio *risk-based*, occorre considerare anche un’altra prospettiva. Occorre, infatti, tenere bene a mente che, almeno per quanto riguarda la regolazione giuslavoristica, i recenti interventi in materia di IA si aggiungono e non si sostituiscono al “patrimonio” di tutele a presidio del prestatore di lavoro, della sua dignità, della sua sicurezza, ecc. Si tratta, dunque, di interventi regolativi volti a identificare rischi nuovi, trasversali a tutti i settori produttivi e a tutti coloro che operano nella società digitale, rispetto ai quali nemmeno il diritto del lavoro ha, e può avere, la presunzione di saper individuare lo strumento regolativo volto ad azzerare tutti i rischi, a meno di non ipotizzare uno stop all’evoluzione digitale certamente non realizzabile. Si tratta, dunque, di anticipare, gestire e mitigare rischi che possono travolgere lo stesso diritto⁽¹⁴⁾ del lavoro che non svanisce, non si liquefa, ma che anzi deve provare a rafforzarsi non solo in funzione rivendicativa di diritti già acquisiti, ma anche in chiave precauzionale e anticipatoria di rischi occulti e/o occultati da algoritmi incomprensibili, sistemi decisionali e di controllo automatizzati e invisibili, ecc.

⁽¹²⁾ M. Barbera, “*La nave deve navigare*”, cit., 3 ss.

⁽¹³⁾ M. Barbera, “*La nave deve navigare*”, cit., 12.

⁽¹⁴⁾ N. Van Dijk - R. Gellert - K. Rommetveit, *A risk to a right? Beyond data protection risk assessments*, *Computer Law & Security Review*, 2016, n. 2, 286 ss.

Si tratta di una sfida di individuazione e di gestione “anticipatoria” di rischi nuovi, rispetto alla quale il diritto del lavoro e i suoi attori – soprattutto quelli collettivi di cui si dirà nelle pagine che seguono – possono e devono giocare un ruolo innovativo, non meramente rivendicativo di diritti già acquisiti nel dna lavoristico, bensì anticipatorio finalizzato all’individuazione di pericoli, anche solo potenziali, insiti nell’utilizzo dei sistemi di IA che possono mettere a rischio i diritti fondamentali dei lavoratori stessi, o che possono indebolire, annullare o vanificare le tutele “tradizionali” già esistenti.

Si tratta, dunque, di una sfida accettabile per il diritto del lavoro a patto, come detto, di considerare la regolazione *risk-based* delle nuove tecnologie come incrementale di tutele già esistenti nella regolazione lavoristica di matrice legale (le norme inderogabili e i principi di non discriminazione) e contrattuale (i diritti di informativa, la contrattazione e il conflitto); una regolazione ulteriore, dunque, che consente di procedere alla individuazione e valutazione di rischi nuovi che mettono a repentaglio l’efficacia regolativa della strumentazione esistente; il tutto tenendo ben salda e orientata la bussola verso i diritti fondamentali e nella consapevolezza di tutti gli attori che la gestione degli nuovi rischi debba servire ad assicurare la permanenza delle tutele o ad aggiungerne di nuove, o a mitigare i rischi di peggioramento delle tutele stesse, e non certo ad indebolire i diritti e le libertà.

3. Le diverse declinazioni del *risk-based approach*: nel GDPR (la prospettiva *bottom-up*)

Il *risk-based approach*, come è noto, è fatto proprio innanzitutto dal GDPR, che impone ai responsabili del trattamento di valutare i rischi che le loro attività di trattamento dei dati comportano e a definire attivamente le misure e le tecniche necessarie per garantire la protezione dei dati individuali e i diritti alla *privacy* in funzione di tali rischi specifici. In tal senso, il GDPR rappresenta la disciplina antesignana della regolazione del rischio per i diritti⁽¹⁵⁾ della persona *tout court*, assurgendo a una sorta meta-regolamentazione fondata sul presupposto che la *privacy* e la protezione dei dati siano i principi guida dello sviluppo tecnologico.

In un’ottica di responsabilizzazione del titolare del trattamento, dunque, il GDPR impone di accertare concretamente il grado di rischio per i diritti fondamentali degli interessati nel trattamento dei dati personali e, sulla base di tale valutazione, a progettare interventi di mitigazione del rischio appropriati. In questa prospettiva, in una logica *bottom-up*⁽¹⁶⁾, il GDPR non stabilisce direttamente la soglia di rischio, ma lascia tale delicato compito agli attori pubblici e privati che sono incaricati del trattamento dei dati

⁽¹⁵⁾ N. Van Dijk - R. Gellert - K. Rommetveit, *A risk to a right?* cit, 286 ss.

⁽¹⁶⁾ G. De Gregorio - P. Dunn, *The European Risk-Based approaches: Connecting Constitutional Dots in The Digital age*, *Common Market Law Review*, 2022, 473 ss.

personali e che, dunque, sono tenuti attraverso una serie di “meta-obblighi”⁽¹⁷⁾ a valutare i rischi⁽¹⁸⁾, e – ove non dimostrino di aver messo in atto misure sufficienti e adeguate a rispettare i principi generali del Regolamento – potranno anche essere chiamati a rispondere della violazione dei diritti degli interessati. Il GDPR delega quindi ai responsabili del trattamento il ruolo fondamentale di individuare da soli i mezzi adeguati per conformarsi ai requisiti di legge. Tale ampio potere, tuttavia, implica un maggior grado di responsabilizzazione del soggetto che esegue il trattamento, atteso che lo stesso è chiamato a rispondere di qualsiasi impatto negativo sui diritti e sulle libertà fondamentali degli interessati. Attraverso tale modello, ai destinatari del GDPR viene concessa una discrezionalità più ampia di quella che sarebbe possibile con un approccio binario *command and control*, ma proprio per questo motivo essi sono resi totalmente responsabili della loro maggiore autonomia e delle loro scelte.

3.1. (segue): nel IA Act (la prospettiva *top-down*)

Un approccio al rischio parzialmente diverso⁽¹⁹⁾ è quello dettato dal IA Act⁽²⁰⁾, nel quale, al fine esplicito di creare un “ecosistema di fiducia”, è lo stesso legislatore che, da una parte, ha effettuato la valutazione preliminare del rischio, in una logica *top-down*⁽²¹⁾, individuando i livelli di rischio alti, come quelli riguardanti l’utilizzo di sistemi di IA nel settore dell’occupazione e nella gestione dei lavoratori⁽²²⁾, o inaccettabili:

⁽¹⁷⁾ A. Aloisi - V. De Stefano, *Between risk mitigation and labour rights enforcement*, cit., 283 ss.

⁽¹⁸⁾ P. Loi, *Il rischio proporzionato nella proposta di regolamento sull’IA e i suoi effetti nel rapporto di lavoro*, cit., 248.

⁽¹⁹⁾ G. Finocchiaro, *La proposta di Regolamento sull’intelligenza artificiale: il modello europeo basato sulla gestione del rischio, Il diritto dell’informazione e dell’informatica*, 2022, n. 2, 303 ss.

⁽²⁰⁾ V. Proposta di Regolamento che stabilisce norme armonizzate sull’intelligenza artificiale del 21 aprile 2021, cosiddetto IA Act, nella versione che dopo l’approvazione del Consiglio è stata ulteriormente emendata nel marzo 2024 dal Parlamento europeo.

⁽²¹⁾ Un diverso modello “misto” è poi quello previsto dal Digital Markets Act (DMA), il nuovo Regolamento europeo sui mercati digitali, approvato dal Parlamento Europeo il 5 luglio 2022 insieme al Digital Services Act (DSA), il Regolamento sui servizi digitali. Le due leggi compongono insieme il Digital Services Package, entrato in vigore nel 2023, che promuove un approccio volto a valutare *ex ante* il rispetto delle regole antitrust, per esempio introducendo un’ampia serie di nuovi obblighi di *due diligence*, quali la trasparenza, *blacklist*, *whitelist*, *case by case assessment*, “per un ambiente online trasparente e sicuro”.

⁽²²⁾ Cfr. il considerando n. 57 il quale espressamente prevede che “i sistemi di IA utilizzati nel settore dell’occupazione, nella gestione dei lavoratori e nell’accesso al lavoro autonomo, in particolare per l’assunzione e la selezione delle persone, per l’adozione di decisioni riguardanti le condizioni del rapporto di lavoro la promozione e la cessazione dei rapporti contrattuali di lavoro, per l’assegnazione dei compiti sulla base dei comportamenti individuali, dei tratti o delle caratteristiche personali e per il monitoraggio o la valutazione delle persone nei rapporti contrattuali legati al lavoro, dovrebbero essere classificati come sistemi ad alto rischio, in quanto tali sistemi possono avere un impatto significativo sul futuro di tali persone in termini di prospettive di carriera e sostentamento e di diritti dei lavoratori. I pertinenti rapporti contrattuali di lavoro dovrebbero coinvolgere, in modo significativo, i dipendenti e le persone che forniscono servizi tramite piattaforme, come indicato nel programma di lavoro annuale della Commissione per il 2021. Durante tutto il processo di assunzione, nonché ai fini della valutazione e della promozione delle persone o del proseguimento dei rapporti contrattuali legati al lavoro, tali

dall'altra, è lo stesso legislatore che – sulla scorta dell'elaborazione dell'High-Level Expert Group on Artificial Intelligence nominato nel 2019⁽²³⁾ – ha identificato i requisiti chiave per l'affidabilità dei sistemi di IA, e quindi per il governo del rischio, basati su principi etici, quali intervento e sorveglianza umana, robustezza tecnica e sicurezza, vita privata e governance dei dati, trasparenza, diversità, non discriminazione ed equità, benessere sociale e ambientale e responsabilità (v. *considerando* n. 27). Nel caso di sistemi di IA ad alto rischio (come appunto quelli utilizzati in materia di occupazione, gestione dei lavoratori e accesso al lavoro autonomo di cui all'allegato III, punto 4), il Regolamento prevede l'adozione di un sistema di gestione dei rischi (art. 9), vale a dire un processo iterativo continuo pianificato ed eseguito nel corso dell'intero ciclo di vita di un sistema di IA ad alto rischio, che richiede un riesame e un aggiornamento costanti e sistematici “di identificazione e analisi dei rischi noti e ragionevolmente prevedibili che il sistema di IA ad alto rischio può porre per la salute, la sicurezza e i diritti fondamentali” e di “adozione di misure di gestione dei rischi opportune e mirate”. Si tratta di un approccio che, inevitabilmente, non tende a eliminare i rischi, ma a ridurli al minimo o al punto tale da considerarli “accettabili” nel bilanciamento con i diritti fondamentali e alla luce dell'applicazione del *test* di proporzionalità²⁴. Un approccio comunque che, tendenzialmente, pur non presupponendo esiti scontati, consente di introdurre a monte una valutazione sulla “tollerabilità” dei rischi imprevedibili sottesi all'utilizzo delle nuove tecnologie ad alta complessità e velocità di cambiamento, quindi nemmeno astrattamente tutti prevedibili per via legislativa.

In questa prospettiva, l'IA Act pone una serie di obblighi di verifica della tollerabilità del rischio sui fornitori, sui distributori e sugli utilizzatori (*deployer*) dei sistemi di IA ad alto rischio; e, allo stesso tempo, a valle dell'utilizzo di tali sistemi – soprattutto per i *deployer* che appunto utilizzano i sistemi stessi in contesti specifici –

sistemi possono perpetuare modelli storici di discriminazione, ad esempio nei confronti delle donne, di talune fasce di età, delle persone con disabilità o delle persone aventi determinate origini razziali o etniche o un determinato orientamento sessuale. I sistemi di IA utilizzati per monitorare le prestazioni e il comportamento di tali persone possono inoltre comprometterne i diritti fondamentali in materia di protezione dei dati e vita privata”. L'art. 6, par. 2, del Regolamento per l'individuazione dei sistemi di IA ad alto rischio rinvia all'allegato III che, al punto 4, include tra i sistemi ad alto rischio, quelli in materia di Occupazione, gestione dei lavoratori e accesso al lavoro autonomo: a) i sistemi di IA destinati a essere utilizzati per l'assunzione o la selezione di persone fisiche, in particolare per pubblicare annunci di lavoro mirati, analizzare o filtrare le candidature e valutare i candidati; b) i sistemi di IA destinati a essere utilizzati per adottare decisioni riguardanti le condizioni dei rapporti di lavoro, la promozione o cessazione dei rapporti contrattuali di lavoro, per assegnare compiti sulla base del comportamento individuale o dei tratti e delle caratteristiche personali o per monitorare e valutare le prestazioni e il comportamento delle persone nell'ambito di tali rapporti di lavoro.

⁽²³⁾ High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI*, 2019. Cfr. L. Floridi, *Establishing the Rules for Building Trustworthy AI*, *Nature Machine Intelligence*, 2019, 261 ss.

⁽²⁴⁾ P. Loi, *Il rischio proporzionato nella proposta di regolamento sull'IA e i suoi effetti nel rapporto di lavoro*, cit., 245.

impone la sorveglianza umana (art. 14) finalizzata a prevenire o ridurre al minimo i rischi per la salute, la sicurezza o i diritti fondamentali che possono emergere quando un sistema di IA ad alto rischio è utilizzato conformemente alla sua finalità prevista o in condizioni di uso improprio ragionevolmente prevedibile, in particolare qualora tali rischi persistano nonostante l'applicazione di altri requisiti previsti nel Regolamento.

Nella logica del IA Act, dunque, la mitigazione del rischio opera a più livelli, con il coinvolgimento di più soggetti, con finalità e principi etici predefiniti, con una strumentazione articolata (sistema di gestione del rischio, trasparenza, sorveglianza umana, valutazione di impatto, ecc.).

3.2. (segue): nella direttiva sul lavoro tramite piattaforme digitali (la prospettiva *command and control* collaborativa)

L'approccio *risk-based* è presente, anche se con modalità ulteriormente diverse, nella proposta di direttiva sul lavoro mediante piattaforme digitali nella versione da ultimo approvata⁽²⁵⁾. La direttiva in corso di approvazione, infatti, prende atto⁽²⁶⁾ dei rischi derivanti da un eccesso di sorveglianza tecnologica, da un accrescimento degli squilibri di potere, dall'opacità del processo decisionale, che – appunto – possono mettere a rischio la sussistenza di condizioni di lavoro dignitose, salute e sicurezza sul lavoro, parità di trattamento e diritto alla riservatezza. A fronte di questi rischi, accanto a tutta una serie di disposizioni finalizzate ad attribuire tutele (quali quelle sulla corretta determinazione della situazione occupazionale, dei meccanismi di presunzione legale, ecc.), la direttiva, da una parte, introduce una serie di misure relative alla gestione algoritmica del lavoro sicuramente riconducibili alla tecnica regolativa *command and control*, vietando alle piattaforme tutta una serie di pratiche ritenute inaccettabili (art. 7); dall'altra, introduce una regolazione procedurale sull'utilizzo dei sistemi decisionali o di monitoraggio automatizzati finalizzata a garantirne la trasparenza (art. 9); dall'altra ancora, all'art. 10, introduce un obbligo di valutazione congiunta “dell'impatto” delle decisioni prese dai sistemi algoritmici che, evidentemente, altro non è che una valutazione dei rischi (verificabili e/o verificati) per le persone, per le loro condizioni di lavoro, sulla parità di trattamento.

Una valutazione del rischio per i diritti, dunque, imposta in una logica *command and control* e, quindi, obbligatoria, ma – allo stesso tempo – pensata come processo “regolare”, almeno biennale, da svolgere “con la partecipazione dei rappresentanti dei

⁽²⁵⁾ Proposta di direttiva COM (2021) 762 del 9 dicembre 2021 relativa al miglioramento delle condizioni di lavoro nel lavoro mediante piattaforme digitali, nella versione approvata dal Consiglio EU l'11 marzo 2024, che ha confermato l'accordo provvisorio sulla direttiva relativa al lavoro mediante piattaforme digitali raggiunto l'8 febbraio 2024 tra la Presidenza del Consiglio e i negoziatori del Parlamento europeo.

⁽²⁶⁾ Considerando n. 4.

lavoratori” e, quindi, in una prospettiva evidentemente “collaborativa”: ove da tale “sorveglianza”/“valutazione” emerga un elevato rischio di discriminazione e/o di violazione dei diritti, la piattaforma sarà tenuta ad adottare le misure necessarie. Non una reale e avvenuta discriminazione, né una reale e avvenuta violazione dei diritti, che chiaramente aprirebbe le porte ad altro tipo di azioni individuali e collettive volte all’accertamento della lesività del comportamento e, ove possibile, alla rimozione degli effetti e/o al risarcimento, bensì un rischio “elevato” del verificarsi di tali situazioni; rischio, quindi, da gestire in una prospettiva collaborativa, ma rispetto al quale la piattaforma sarà tenuta ad adottare le misure necessarie per evitare, nel futuro, che vengano adottate altre decisioni automatizzate ugualmente “rischiose”.

4. *Rights-based versus risk-based approach: quale ruolo per il sindacato?*

Che l’inafferrabilità dei nuovi contesti lavorativi affollati da tecnologie tanto più intelligenti, quanto incomprensibili, il solipsismo del lavoro *online*, la frammentazione interna ed esterna del lavoro subordinato, la destrutturazione dei settori produttivi e la forte disomogeneità della “folla” di lavoratori digitali intermediati da piattaforme, siano tutti fenomeni che mettano duramente alla prova i soggetti collettivi è dato inconfutabile⁽²⁷⁾. Che questa evoluzione determini la fine della stagione della intermediazione degli attori collettivi è tuttavia ipotesi catastrofista lungi dall’essere vicina all’avverarsi. Il processo di digitalizzazione, infatti, pone il sindacato non solo di fronte a inedite difficoltà di spinta dell’associazionismo sindacale e di raccolta di istanze differenziate e rarefatte, ma anche nuove possibilità di rilancio del ruolo del sindacato stesso⁽²⁸⁾, della rappresentanza collettiva dei lavoratori digitali⁽²⁹⁾, della contrattazione⁽³⁰⁾ e della partecipazione⁽³¹⁾, se non di trasformazione dell’impresa in un

⁽²⁷⁾ P. Tullini, *L’economia digitale alla prova dell’interesse collettivo*, LLI, 2018, n. 1, 4 ss.

⁽²⁸⁾ B. Caruso, *Il sindacato tra funzioni e valori nella “grande trasformazione”. L’innovazione sociale in sei tappe*, in B. Caruso - R. Del Punta - T. Treu (a cura di), *Il diritto del lavoro e la grande trasformazione*, Bologna, 2020, 145 ss.

⁽²⁹⁾ W. Chiaramonte, *Lavoro (povero) tramite piattaforme digitali, rappresentanza e tutela collettiva fra sindacalismo informale e sindacalismo tradizionale*, in L. Chies - M.D. Ferrara - E. Podrecca (a cura di), *Le dimensioni della povertà*, Torino, 2021, 263 ss.; C. Faleri, *Brevi spunti di riflessione sull’evoluzione delle relazioni sindacali nell’economia digitale*, *Ianus DF*, 2021, n. 24, 93 ss.; G. Recchia, *Alone in the crowd? La rappresentanza e l’azione collettiva ai tempi della Sharing Economy*, *RGL*, 2018, n. 1, 144 ss.; M. Forlivesi, *Interessi collettivi e rappresentanza dei lavoratori del web*, in P. Tullini (a cura di), *Web e lavoro. Profili evolutivi e di tutela*, Torino, 2017, 192 ss.; A. Lassandari, *La tutela collettiva del lavoro nelle piattaforme digitali: gli inizi di un percorso difficile*, LLI, 2018, n. 1, IV ss.; M. Magnani, *Nuove tecnologie e diritti sindacali*, LLI, 2019, n. 2, 3 ss.; J. Prassl, *Collective Voice in the Platform Economy: Challenges, Opportunities, Solution*, Report to the ETUC, 2018.

⁽³⁰⁾ J.M. Miranda Boto - E. Brameshuber - P. Loi - L. Ratti (a cura di), *Contrattazione Collettiva e gig economy. Uno strumento tradizionale per nuovi modelli di organizzazione*, Torino, 2022; M. Lamannis, *Collective bargaining in the platform economy: a mapping exercise of existing initiatives*, ETUI, 2023.

⁽³¹⁾ Per alcuni recenti riferimenti al tema si rinvia A. Alaimo, *I nuovi termini del discorso giuridico sulla partecipazione dei lavoratori. Partecipazione organizzativa e diretta versus partecipazione indiretta: per una dialettica*

vero e proprio modello di “impresa partecipata” di ispirazione olivettiana, quale luogo in cui sviluppare prassi collaborative non solo per aumentare la produttività e massimizzare, per gli azionisti, il valore prodotto e l’utile da distribuire, ma sempre più spesso per obiettivi di sostenibilità sociale e ambientale⁽³²⁾.

Al di là degli accennati percorsi virtuosi, è però evidente come si è detto che il processo di digitalizzazione possa anche dare vita a nuove pervasive forme di controllo e di assoggettamento da parte del cosiddetto *management algoritmico*, e dunque a nuove forme di rischio per i diritti, finendo per calcificare pregiudizi, disuguaglianze e stereotipi, aumentando disparità, imprecisioni e arbitrarietà. È proprio sul fronte delle tecniche di utilizzo dei sistemi di intelligenza artificiale nella gestione delle risorse umane che già l’Accordo quadro delle Parti Sociali sulla Digitalizzazione del giugno 2020 prende atto dei rischi connessi alla diffusione di tali sistemi, a fronte dei quali evidenzia come sia fondamentale per le parti sociali assicurarsi che i sistemi medesimi non compromettano, bensì aumentino, il coinvolgimento umano e le capacità sul lavoro⁽³³⁾.

senza contrapposizione, WP CSDLE “Massimo D’Antona”.IT – 480/2024; L. Zoppoli, *La partecipazione sindacale nella civiltà digitale*, DRI, 2023, 958 ss.

⁽³²⁾ B. Caruso, *Impresa partecipata e contratto di lavoro*, WP CSDLE “Massimo D’Antona”.IT – 484/2024; per una analisi del percorso virtuoso di coinvolgimento del sindacato, quale soggetto in grado non solo di accompagnare i cambiamenti tecnologici, avendo come stella polare una prospettiva di collaborazione strategica (che mette in secondo piano il conflitto), ma anche di curvare l’impatto sistemico degli stessi a beneficio di tutti si rinvia a R. Del Punta, *Un diritto del lavoro 4.0*, in A. Cipriani - A. Grimolati - G. Mari (a cura di), *Il lavoro 4.0. La quarta rivoluzione industriale e le trasformazioni delle attività lavorative*, Firenze, 2018, 224 ss.; M. Carrieri, F. Pirro, *Digitalizzazione, relazioni industriali e sindacato. Non solo problemi, ma anche opportunità*, in A. Cipriani - A. Grimolati - G. Mari (a cura di), *Il lavoro 4.0. La quarta rivoluzione industriale e le trasformazioni delle attività lavorative*, cit., 131 ss. Sul ruolo del sindacato come soggetto in grado di adattarsi al nuovo modo di produzione dell’Industria 4.0, sino a proporsi come risorsa strategica, anche di governo, dell’impresa v. B. Caruso, R. Del Punta, T. Treu, *Manifesto per un diritto del lavoro sostenibile*, in CSDLE “Massimo D’Antona”, 2020, 53 ss. Sebbene l’ambivalenza delle ricadute dell’utilizzo dei sistemi di intelligenza artificiale sulle relazioni sindacali sia stata confermata anche dalle più recenti indagini internazionali, le indagini stesse evidenziano come l’adozione di tecnologie con componenti di intelligenza artificiale nelle aziende che hanno, al proprio interno, forme di rappresentanza dei lavoratori sia significativamente associata a migliori condizioni di lavoro rispetto all’adozione degli stessi sistemi da parte di aziende in cui non vi siano relazioni sindacali collaborative, v. OECD *Employment Outlook 2023: Artificial Intelligence and the Labour Market*, OECD Publishing, 2023, par. 7.

⁽³³⁾ Si tratta di un Accordo quadro autonomo di tipo bilaterale che, a fronte della sfida apportata dall’economia digitale *multifaced topic*, invita gli attori sindacali operanti in ambito europeo a stimolare, a tutti i livelli, un processo dinamico circolare in grado di realizzare una transizione digitale consensuale, di cogliere le opportunità, nonché di prevenire e ridurre al minimo i rischi, garantendo il miglior risultato possibile sia per i datori di lavoro, sia per i lavoratori. Su tale accordo v. T. Treu, *La digitalizzazione del lavoro: proposte europee e piste di ricerca*, in *federalismi.it*, 2022, n. 9, 190 ss.; C. Faleri, *Brevi spunti di riflessione sull’evoluzione delle relazioni sindacali nell’economia digitale*, cit., 108 ss.; A. Rota, *Sull’Accordo quadro europeo in tema di digitalizzazione del lavoro*, LLI, 2020, n. 2, 25 ss.; M. Peruzzi, *Il dialogo sociale di fronte alle sfide della digitalizzazione*, DRI, 2020, 1213 ss.; G. Pigni, *European Social Partners Framework Agreement on digitalisation: ottimizzare i benefici ed affrontare insieme le sfide della digitalizzazione*, BA, 2020, n. 26; I. Purificato, *Governare l’innovazione tecnologica: il rilancio del metodo partecipativo in rapporto sinergico con la contrattazione collettiva*, *Quaderno della Rivista Diritti Lavori Mercati*, 2023, 121 ss.; L. Imberti, *Intelligenza artificiale e sindacato. Chi controlla i controllori artificiali?* *federalismi.it*, 2023, n. 29, 192 ss.

È in questa prospettiva che il sindacato può e deve candidarsi a svolgere un ruolo chiave, non solo in funzione rivendicativa di diritti esistenti, secondo un approccio “tradizionale” *rights-based*, ma anche in funzione di attore tecnologicamente alfabetizzato, attivo e propositivo, in grado di intraprendere un percorso, difficile, ma non impossibile, di progressiva comprensione delle nuove tecnologie, dei nuovi sistemi di IA, delle nuove fattispecie di lavoro tramite piattaforma *sans phrase*⁽³⁴⁾, di analisi e valutazione dei rischi ad essi connessi, nonché di mitigazione dei rischi insiti nel loro utilizzo: ciò nella consapevolezza che proprio sul terreno sindacale e con gli strumenti di intervento vecchi e nuovi a disposizione degli attori collettivi possa essere attuato un bilanciamento *win win* tra IA e diritti sociali⁽³⁵⁾.

È noto come l’approccio antropocentrico, sia considerato il baluardo del modello europeo, sia nella sua declinazione etica, sia in quella giuridica, basata sul sistema di sorveglianza umana; la scelta etica e giuridica della legislazione europea in materia sembra, dunque, quella di porre al centro dello sviluppo del mercato digitale europeo l’individuo, la persona umana, non solo come limite alla tecnologia quando questa intacca i diritti fondamentali, ma anche e soprattutto come attore che deve restare protagonista del sistema, quale portatore di una permanente e ineliminabile alternativa di razionalità umana, di capacità di analisi dei fatti e dei contesti (e non solo dei dati) che deve restare centrale nell’utilizzo dei sistemi di IA. L’inafferrabilità dell’approccio antropocentrico e della sorveglianza umana apre ovviamente problemi giuridici, interpretativi e applicativi enormi; pare inevitabile ipotizzare come, infatti, l’approccio antropocentrico sia ben lontano dall’evocare una prospettiva di “individualismo tradizionale”, in base al quale l’individuo libero si pone al centro delle proprie scelte e si autodetermina dal punto di vista tecnologico. Piuttosto, è da condividere la lettura secondo la quale la sfida e l’ambizione europea che deve essere coltivata è nel senso di sviluppare una nuova idea di “individualismo collettivo” che sta alla base dell’approccio antropocentrico, vale a dire di una individualità/umanità collettivamente intesa, portatrice del progetto di integrazione europea, dei valori dell’Unione e dei diritti fondamentali e che possa agire “collettivamente” a presidio di una sviluppo tecnologico che resti antropocentrico⁽³⁶⁾.

Se così è, come si ritiene debba essere, è ovvio che nell’ambito delle relazioni di lavoro il soggetto storicamente titolato a porsi come portatore di interessi collettivi delle persone che operano nei luoghi di lavoro e per una gestione dei rapporti che resti governata da una razionalità umana è proprio il sindacato, che dunque – nella nuova partita della gestione dei rischi connessi all’utilizzo di sistemi di IA – può e deve giocare

⁽³⁴⁾ L. Zappalà, *Vulnerabili digitali, poveri della rete e padroni del tempo: l’approccio rimediale case-by-case nel lavoro delle piattaforme*, in B. Caruso (a cura di), *Il lavoro povero sans phrase*, Bologna, 2024, 283 ss.

⁽³⁵⁾ P. Loi, *Il rischio proporzionato nella proposta di regolamento sull’IA e i suoi effetti nel rapporto di lavoro*, cit., 251.

⁽³⁶⁾ M. Catanzariti, *Rischio e vulnerabilità nel modello europeo di intelligenza artificiale*, cit., 81.

un ruolo centrale a presidio dello sviluppo di un modello di IA che sia affidabile, per l'uomo, e che resti appunto antropocentrica.

5. Il possibile contributo “a monte” del sindacato nella valutazione *risk-based*: a) del trattamento automatizzato (e non) dei dati

Un significativo, ma forse ancora poco sviluppato, ruolo degli attori collettivi nel governo delle tecnologie può essere innanzitutto giocato “a monte” dell'introduzione delle stesse, nella fase prodromica di valutazione dell'impatto e di valutazione del rischio connesso soprattutto all'utilizzo di sistemi di intelligenza artificiale.

Nel solco del *risk-based approach*, l'art. 35, par. 1, del GDPR, stabilisce l'obbligo per il titolare di effettuare, prima dell'inizio del trattamento, una valutazione dell'impatto del trattamento medesimo (DPIA), laddove quest'ultimo possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

La tecnica regolativa della valutazione di impatto, già sperimentata per esempio per la valutazione di impatto ambientale, è utilizzata, come sopra accennato, per valutare – in una logica anticipatoria – i rischi sui diritti e sulle libertà delle persone; valutazione di impatto che, secondo il par. 9, dell'art. 35 citato, il titolare del trattamento può fare raccogliendo le opinioni degli interessati o dei loro rappresentanti. Nell'ottica di una maggiore responsabilizzazione del soggetto regolato⁽³⁷⁾, la regolazione *risk-based* cui si si ispira il GDPR presuppone e si fonda su una architettura collaborativa, nella quale il titolare del trattamento è chiamato a valutare, insieme agli *stakeholders*, i rischi per i diritti e le libertà delle persone fisiche. È questa la sede, dunque, in cui gli interessati possono esercitare l'opzione *voice*, dapprima comprendendo in cosa consista il trattamento, e di conseguenza in via preventiva e precauzionale evidenziando i rischi (anche soltanto eventuali) per i diritti e le libertà.

Fra le tipologie di trattamenti soggetti al requisito di una valutazione d'impatto figurano i trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione)⁽³⁸⁾ dai quali derivi la possibilità di effettuare un controllo a distanza

⁽³⁷⁾ G. De Gregorio - P. Dunn, *The European Risk-Based approaches*, cit., 482.

⁽³⁸⁾ Come chiarito dal Garante per la protezione dei dati personali, con il Provvedimento n. 467 del 2018, Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679 - 11 ottobre 2018. Il chiarimento del Garante, in particolare, richiama le Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento “possa presentare un rischio elevato” ai fini del Regolamento (UE) 2016/679 del Gruppo di Lavoro Articolo 29 per la Protezione dei Dati del 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 e fatte proprie dal Comitato europeo per la protezione dei dati il 25 maggio 2018, che hanno individuato una serie di criteri, tutti di rilevanza lavoristica, da tenere in considerazione ai fini dell'identificazione dei trattamenti che possono presentare un “rischio elevato” (quali per esempio la valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione, in particolare in considerazione di “aspetti riguardanti

dell'attività dei dipendenti, come più in generale i trattamenti automatizzati finalizzati ad assumere decisioni che producono “effetti giuridici” oppure che incidono “in modo analogo significativamente” sull'interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere, nonché i trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. *IoT*; sistemi di intelligenza artificiale; utilizzo di assistenti vocali online attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi *wearable*; tracciamenti di prossimità, ecc.).

Nonostante gli spazi aperti dal GDPR alle rappresentanze dei lavoratori nella DPIA⁽³⁹⁾, che potrebbero quindi avere contezza “a monte” del rispetto delle regole della necessaria sorveglianza umana sui sistemi automatizzati, della robustezza e accuratezza del trattamento, ecc. non risultano prassi consolidate di coinvolgimento degli attori collettivi nella gestione del *design* del trattamento dei dati e dei sistemi decisionali automatizzati e non. Vero è che la previsione citata non prevede un vero e proprio obbligo di consultazione delle rappresentanze sindacali, quanto una possibilità di procedere alla stessa, ma è anche vero – come chiarito dalle Linee-guida del Gruppo Articolo 29 in materia di valutazione di impatto sulla protezione dei dati – che il principio di responsabilizzazione (*accountability*) deve essere inteso nel senso di imporre l'obbligo di indicare nella DPIA le ragioni per le quali non è stato chiesto il parere agli interessati o ai loro rappresentanti, o il perché ci si sia discostati dall'opinione ricevuta, motivando le ragioni di ogni scelta. In ragione di tale apertura, gli spazi per un intervento proattivo del sindacato volto alla individuazione e valutazione dei rischi sui diritti e sulle libertà dei lavoratori avrebbero potuto essere ben maggiori, così come la rivendicazione di iniziative, collettive o a supporto di istanze individuali, volte a comprendere le modalità di trattamento dei dati, nonché a minimizzarne i rischi a protezione della dignità dei lavoratori coinvolti.

L'assenza di interesse degli attori collettivi, almeno sul piano nazionale, per l'approccio valutativo “a monte” *risk based*, forse è giustificabile alla luce della sussistenza nel nostro ordinamento di una disposizione in materia di controlli datoriali molto più “incisiva”, e tipizzata in chiave di controllo *hard*, qual è l'art. 4 dello Statuto dei lavoratori, richiamato dallo stesso art. 114 del Codice della *privacy*; ma è pur vero che il disinteresse per tale modalità di coinvolgimento è emblematico della mancanza di una cultura sindacale sulla gestione dei rischi per i diritti (essendo fisiologicamente e storicamente il

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”; il processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente sulle persone; il monitoraggio sistematico degli interessati; ecc.).

⁽³⁹⁾ M. Peruzzi, *Intelligenza artificiale e lavoro*, cit., 59 ss.; A. Ingraio, *Il controllo a distanza sui lavoratori e la nuova disciplina privacy. Una lettura integrata*, Cacucci, 2018., 133 ss.

sindacato abituato a rivendicare i diritti, e non a prevenire i rischi per i diritti stessi), ma anche di una scarsa lungimiranza degli attori collettivi che, iniziando a capire come vengono utilizzati i dati, avrebbero potuto e potrebbero capire “a monte” cosa il datore di lavoro può dare in pasto agli algoritmi decisionali.

5.1. (segue): b) nei casi di utilizzo di sistemi di intelligenza artificiale ad alto rischio

Un approccio parzialmente differente sembra invece emergere dalla lettura dell’ultima versione dell’IA Act del marzo 2024 che, da una parte, ha previsto all’art. 26, par. 7 per i *deployer* che sono datori di lavoro⁽⁴⁰⁾ e che utilizzano sistemi di IA ad alto rischio l’obbligo, prima della messa in servizio o dell’utilizzo di un sistema di IA ad alto rischio sul luogo di lavoro, di informare i rappresentanti dei lavoratori e i lavoratori interessati che saranno assoggettati a tale sistema di IA. Si tratta di un obbligo di informativa apparentemente più blando di quello originariamente previsto nella versione proposta dal Parlamento europeo (che richiedeva espressamente ai datori di lavoro di consultare i rappresentanti dei lavoratori al fine di raggiungere un accordo in conformità con la direttiva 2002/14/CE), ma che comunque specifica che le informazioni debbano essere fornite conformemente alle norme e alle procedure stabilite dal diritto e dalle prassi dell’Unione e nazionali in materia di informazione dei lavoratori e dei loro rappresentanti e che non esclude, dunque, la possibilità di un approccio partecipativo significativo del soggetto sindacale.

Il successivo art. 27 del medesimo testo regolamentare, poi, prevede l’obbligo dei *deployer* di procedere a una valutazione d’impatto sui diritti fondamentali per i sistemi di IA ad alto rischio. Come chiarito dal *considerando* n. 96, l’obiettivo della valutazione d’impatto sui diritti fondamentali è consentire al *deployer* di individuare i rischi specifici per i diritti delle persone o dei gruppi di persone che potrebbero essere interessati e di individuare le misure da adottare al concretizzarsi di tali rischi. Tale valutazione, come chiarito del medesimo *considerando* n. 96, dovrebbe individuare i processi pertinenti del *deployer* in cui il sistema di IA ad alto rischio sarà utilizzato in linea con la sua finalità e dovrebbe includere una descrizione del periodo di tempo in cui il sistema è destinato a essere usato e della relativa frequenza, nonché delle categorie specifiche di persone fisiche e gruppi che potrebbero essere interessati nel contesto specifico di utilizzo⁽⁴¹⁾. Si

⁽⁴⁰⁾ Per una analisi dettagliata degli obblighi del *deployer*, si rinvia a M. Peruzzi, *Intelligenza artificiale e lavoro: l’impatto dell’AI Act nella ricostruzione del sistema regolativo e di tutela*, in M. Biasi (a cura di), *Diritto del lavoro e intelligenza artificiale*, Giappichelli, 2024, 115 ss.

⁽⁴¹⁾ Il *considerando* n. 96 chiarisce ancora che «La valutazione dovrebbe altresì comprendere l’individuazione di rischi specifici di danno che possono incidere sui diritti fondamentali di tali persone o gruppi. Nell’effettuare tale valutazione, il *deployer* dovrebbe tenere conto delle informazioni pertinenti per un’adeguata valutazione dell’impatto, comprese, tra l’altro, le informazioni trasmesse dal fornitore del sistema di IA ad alto rischio nelle istruzioni per l’uso. Alla luce dei rischi individuati, i *deployer*

tratta, insomma di una vera e propria co-progettazione della procedura di individuazione e gestione del rischio che, evidentemente, potrebbe aprire spazi di controllo per il sindacato di rilevante portata strategica.

L'art. 27 del Regolamento, tuttavia, da una parte, inspiegabilmente, limita la valutazione d'impatto medesima solo ad alcuni casi di utilizzo di sistemi ad alto rischio (escludendo dall'elenco quelli contenuti nell'Allegato III, par. 4, vale a dire quelli utilizzati per l'assunzione e la selezione e quelli utilizzati per adottare decisioni riguardanti le condizioni dei rapporti di lavoro, la promozione o cessazione dei rapporti contrattuali di lavoro, per assegnare compiti sulla base del comportamento individuale o dei tratti e delle caratteristiche personali o per monitorare e valutare le prestazioni e il comportamento delle persone nell'ambito di tali rapporti di lavoro); dall'altra, al successivo par. 4 del medesimo art. 27, prevede una sorta di rinvio al GDPR, stabilendo che se uno qualsiasi degli obblighi di cui all'articolo in questione sia già rispettato a seguito della valutazione d'impatto sulla protezione dei dati effettuata a norma dell'articolo 35 del GDPR, la valutazione d'impatto sui diritti fondamentali di cui al par. 1 (dell'art. 27 del IA Act) integra tale valutazione d'impatto sulla protezione dei dati.

La formulazione non pare essere delle più felici, ma probabilmente l'intento del legislatore europeo era solo quello di evitare (in alcuni casi) una possibile "duplicazione" di valutazioni di impatto: per ciò si è stabilito che laddove il *deployer* sia già tenuto a eseguire una valutazione di impatto sui dati personali (come nel caso del trattamento dei dati sui luoghi di lavoro) la valutazione dell'impatto sulla protezione dei dati e quella sui diritti fondamentali debbano coincidere. Nel nuovo testo del IA Act, dunque, la valutazione d'impatto sui diritti fondamentali dei sistemi ad alto rischio utilizzati nei luoghi di lavoro, lungi dall'essere eliminata, è stata solo accorpata alla valutazione di impatto prevista dall'art. 35 del GDPR⁽⁴²⁾.

dovrebbero stabilire le misure da adottare al concretizzarsi di tali rischi, compresi, ad esempio, i meccanismi di *governance* in tale contesto specifico di utilizzo, quali le modalità di sorveglianza umana secondo le istruzioni per l'uso, o le procedure di gestione dei reclami e di ricorso, dato che potrebbero essere determinanti nell'attenuare i rischi per i diritti fondamentali in casi d'uso concreti. Dopo aver effettuato tale valutazione d'impatto, il *deployer* dovrebbe darne notifica alla pertinente autorità di vigilanza del mercato. Se del caso, per raccogliere le informazioni pertinenti necessarie a effettuare la valutazione d'impatto, i *deployer* di sistemi di IA ad alto rischio, in particolare quando i sistemi di IA sono utilizzati nel settore pubblico, potrebbero coinvolgere i portatori di interessi pertinenti, compresi i rappresentanti di gruppi di persone che potrebbero essere interessati dal sistema di IA, gli esperti indipendenti e le organizzazioni della società civile nello svolgimento di tali valutazioni d'impatto e nella progettazione delle misure da adottare al concretizzarsi dei rischi».

⁽⁴²⁾ Tale lettura, del resto, sembra supportata dal testo della precedente versione dell'AI Act, il quale all'art. 29a, nel prevedere regole specifiche sulla valutazione dell'impatto sui diritti fondamentali per i sistemi di intelligenza artificiale ad alto rischio, stabiliva – al par. 4 – che, laddove la valutazione d'impatto dei sistemi ad alto rischio, fosse stata oggetto anche di una valutazione d'impatto sulla protezione dei dati condotta ai sensi dell'art. 35 del GDPR (che, come si è detto, prevede anche il coinvolgimento dei rappresentanti dei lavoratori o la motivazione della loro mancata consultazione) le due valutazioni avrebbero dovuto essere condotte congiuntamente; *v.* sul punto M. Peruzzi, *Intelligenza artificiale e lavoro*, cit., 65 ss.

Molti dei *considerando* del Regolamento, del resto, supportano tale lettura: il *considerando* n. 48 collega direttamente la “portata dell’impatto negativo” dei sistemi di IA ad alto rischio sui diritti fondamentali, quali il diritto alla dignità umana, il rispetto della vita privata e della vita familiare, la protezione dei dati personali, la libertà di espressione e di informazione, la libertà di riunione e di associazione e la non discriminazione, i diritti dei lavoratori, i diritti delle persone con disabilità e l’uguaglianza di genere; il *considerando* n. 48, a proposito dei sistemi di IA ad alto rischio utilizzati nei settori dell’occupazione, nella gestione dei rapporti di lavoro e nell’accesso al lavoro autonomo riconosce espressamente la possibilità di impatto significativo sui diritti fondamentali; il *considerando* n. 65 richiama la necessità del sistema di gestione rischi da applicare nel corso dell’intero ciclo di vita di un sistema di IA ad alto rischio volto a individuare e attenuare i rischi per i diritti fondamentali di cui il *deployer* dovrebbe essere consapevole, in quanto soggetto che appunto utilizza i sistemi in un contesto specifico (*considerando* n. 93).

Alla luce del testo complessivo, sarebbe, pertanto, del tutto illogico che proprio nell’ambito dei rapporti di lavoro – sicuramente uno degli ambiti di utilizzo dei sistemi di IA ad alto rischio che più rischiano di impattare, per ammissione stessa del Regolamento, sui diritti fondamentali – il *deployer* non sia tenuto a una valutazione di impatto che coinvolga i rappresentanti sindacali, quali soggetti sicuramente in grado di portare dentro la valutazione quella prospettiva antropocentrica su cui si fonda il modello europeo di regolazione della IA affidabile.

È, pertanto, logico e auspicabile che le rappresentanze dei lavoratori chiamate a partecipare alla valutazione dell’impatto sulla protezione dei dati, vengano coinvolte anche nella valutazione d’impatto dei sistemi di IA ad alto rischio sui diritti fondamentali, e dunque in uno spazio d’azione e di valutazione di sicuro maggiore interesse per gli attori collettivi. Ciò conferma come gli attori collettivi, da subito, nelle more dell’entrata in vigore del AI Act e nelle more della adozione definitiva della direttiva sul lavoro tramite piattaforme (v. *infra*), dovrebbero già iniziare a “imporsi” come interlocutori seri, alfabetizzati e proattivi del *risk-based approach*, che dai dati potrebbero apprestarsi a valutare anche il più dirompente impatto sui diritti fondamentali dei lavoratori dei luoghi di lavoro digitalizzati.

5.2. (segue): c) nella valutazione di impatto sui sistemi automatizzati utilizzati dalle piattaforme di lavoro

L’occasione, fino ad ora, persa dagli attori collettivi di intervenire “a monte” sul processo di organizzazione del trattamento dei dati e sulle modalità di utilizzo dei sistemi decisionali automatizzati potrebbe ripresentarsi ai sindacati, oltre che a seguito dell’approvazione del IA Act di cui si è detto, anche a seguito dell’ormai imminente varo

della direttiva sul lavoro mediante piattaforme digitali nella versione da ultimo approvata di cui si è detto sopra.

Particolarmente significativa si rivela, infatti, la previsione della direttiva sul lavoro tramite piattaforme, che – all’art. 8 – istituisce un preciso obbligo per le piattaforme di lavoro di effettuare la valutazione di impatto dell’art. 35, par. 1, del GDPR e di chiedere il parere delle persone che svolgono un lavoro mediante piattaforme digitali e dei loro rappresentanti, nonché l’obbligo (evidentemente successivo) di fornire la valutazione d’impatto medesima, nella versione finale redatta, ai rappresentanti dai lavoratori.

In sintesi, mentre il GDPR si limita a prevedere la possibilità per il titolare del trattamento di “raccolgere le opinioni degli interessati e dei loro rappresentanti”, la direttiva sul lavoro tramite piattaforma si appresta a trasformare tale possibilità in un vero e proprio obbligo di chiedere il parere dei rappresentanti dei lavoratori che, quindi, verranno sempre più coinvolti “a monte” nel processo di comprensione dell’impatto dei sistemi decisionali e di monitoraggio automatizzati gestiti dalle piattaforme di lavoro medesime. Il coinvolgimento delle rappresentanze dei lavoratori nella valutazione di impatto dei sistemi automatizzati è poi affiancato da un più generale obbligo di informazione e consultazione sindacale (previsto dal successivo art. 13 della direttiva in corso di approvazione) sulle decisioni che possono comportare l’introduzione di un sistema decisionale automatizzato o una modifica sostanziale al suo utilizzo.

Per rendere effettiva e consapevole la partecipazione sindacale, si prevede poi che i rappresentanti dei lavoratori delle piattaforme digitali possano essere assistiti da un esperto di loro scelta, nella misura in cui ciò sia loro necessario per esaminare la questione oggetto di informazione e consultazione e formulare un parere. La presenza di tale esperto, dunque, potrà giocare un ruolo fondamentale nel garantire una partecipazione sindacale attiva e consapevole, sia appunto nella citata fase di informativa, sia in sede di valutazione di impatto sulla protezione dei dati, sia pure nella fase della valutazione di impatto sulle condizioni di lavoro, che – senza dubbio – rappresenta la porta d’ingresso “sindacale” per garantire una reale “sorveglianza” umana sui potenziali rischi di discriminazione e/o di violazione dei diritti della persona gestita da algoritmi.

Un ulteriore specifico spazio d’azione per gli attori collettivi è poi previsto dall’art. 10 prima citato del testo di direttiva sul lavoro tramite piattaforme digitali nella versione approvata nel marzo scorso: tale articolo, come sopra accennato, espressamente stabilisce l’obbligo per gli Stati membri di garantire la sorveglianza umana sui sistemi automatizzati, anche prevedendo – almeno ogni due anni – una valutazione d’impatto, svolta congiuntamente dalla piattaforma e dai rappresentanti dei lavoratori, delle decisioni individuali prese o sostenute dai sistemi decisionali o di monitoraggio automatizzati utilizzati sulle persone che svolgono un lavoro mediante piattaforme digitali, incluso, se del caso, sulle loro condizioni di lavoro e sulla parità di trattamento

sul lavoro. Laddove, quindi, la piattaforma utilizzi sistemi automatizzati, la disciplina europea in fase di approvazione definitiva prevede una procedura di “monitoraggio” continuo degli effetti delle decisioni prese dai sistemi automatizzati, nella quale i sindacati saranno chiamati sia a partecipare attivamente alla valutazione d’impatto sulle condizioni di lavoro, sia a ricevere le informazioni “finali” sulla valutazione d’impatto medesima effettuata. La partecipazione dei rappresentanti dei lavoratori al processo di valutazione dei rischi discendenti dall’utilizzo dei sistemi automatizzati da parte delle piattaforme di lavoro si scinde, dunque, in due fasi: una prima fase, riguardante la valutazione d’impatto sulla protezione dei dati (*ex art. 8*), e una valutazione d’impatto almeno biennale degli specifici effetti dell’utilizzo dei sistemi automatizzati sul rapporto di lavoro (*ex art. 10*), che potenzialmente eleva – di fatto – il sindacato al ruolo attivo di “sorvegliante umano” del *management* algoritmico.

Tale coinvolgimento potrebbe avere l’effetto di attribuire al sindacato un ruolo strategico sia nel veicolare nel descritto processo di valutazione logiche antropocentriche, ma anche e soprattutto nel monitorare i rischi per i diritti dei lavoratori, segnalando la necessità di interventi correttivi, ove si tratti di rischi “potenziali”; o ponendo in essere azioni rivendicative “tradizionali” dei diritti lesi, nel caso in cui il rischio, da possibile, si sia tramutato in una vera e propria lesione dei diritti dei lavoratori e/o dello stesso sindacato stabiliti da norme di legge e/o di contratto collettivo.

6. La trasparenza come veicolo di emersione dei rischi per i diritti

“A valle” della fase inerente le scelte organizzative aziendali relative all’introduzione dei sistemi di intelligenza artificiale e del potenziale ruolo degli attori sociali di cui si è detto, si stagliano i nuovi diritti individuali e collettivi di ottenere informazioni chiare, trasparenti e comprensibili sull’utilizzo dei sistemi automatizzati da parte del datore di lavoro. Il problema della trasparenza⁽⁴³⁾ della decisione algoritmica è, già da qualche tempo, al centro del dibattito delle istituzioni europee, sotto diversi profili, spesso utilizzato quale viatico di una più ampia strategia di sostenibilità dell’attività d’impresa⁽⁴⁴⁾, che passa anche attraverso la chiarezza delle informazioni rese ai lavoratori, alle loro rappresentanze e, più in generale, ai portatori di interessi.

È ampiamente studiato come il ruolo della trasparenza nel diritto del lavoro sia sfaccettato avendo gli ormai numerosi obblighi di informativa, soprattutto quelli di “terza generazione”, non solo una funzione comunicativa, ma anche una funzione

⁽⁴³⁾ Sul punto si rinvia a L. Zappalà, *Transparency and comprehensibility of working conditions and automated decisions: is it possible to open the black box? The Italian Law Journal*, 2023, n. 2.

⁽⁴⁴⁾ C. Faleri, *Diritti di informazione e principio di trasparenza per una governance societaria sostenibile*, *LD*, 2023, n. 3, 545 ss.; sul tema pure v. V. Brino, *La governance societaria sostenibile: un cantiere da esplorare per il diritto del lavoro? LD*, 2023, n. 3, 445 ss.

commutativa del linguaggio delle macchine, che – anche in altri campi del diritto – sta aprendo le porte al dibattito sulla *fairness algoritmica* e sulla *Corporate Digital Responsibility*⁽⁴⁵⁾, quale veicolo per la ricerca di un punto di equilibrio antropocentrico tra apporto automatizzato e fattore umano, ossia tra razionalità della macchina e pensiero gestionale umano. La trasparenza, sempre più declinata in una pluralità di diritti/doveri di informazione ormai presenti in diversi ambiti regolativi in questa sede non riepilogabili, ha così assunto il ruolo di principio trasversale in grado di veicolare tutele universali dentro e oltre la fattispecie, assurgendo a nuovo paradigma del diritto del lavoro che, nonostante i suoi limiti e le sue fragilità, mira sempre più ad affermare modello di *governance* delle informazioni che colma le asimmetrie uomo/sindacato-macchina, aprendo spazi di maggiore comprensione per tutti gli attori coinvolti nell'utilizzo di sistemi di IA ad alto rischio sul come funzionino tali sistemi decisionali automatizzati e quali rischi comportino per lavoratori, diritti e libertà.

La trasparenza è, pertanto, al centro della regolazione europea, nella consapevolezza che per essere antropocentrica l'IA deve essere innanzitutto compresa nelle sue modalità di funzionamento: la trasparenza, veicola la conoscenza e la comprensibilità e, di conseguenza, consente di valutare i rischi dell'utilizzo dei sistemi di IA ad alto rischio.

La trasparenza, dunque, fra le sue molteplici funzioni (ivi compresa quella abilitativa del singolo di comprendere come vengano elaborati e trattati i suoi dati, come venga ricostruita la sua identità dagli algoritmi) ha anche una plurima funzione abilitativa che consente l'esercizio individuale e collettivo di diritti già posti da norme inderogabili e da disposizioni collettive (per esempio consente di capire come funziona un sistema di controllo della prestazione ai fini di valutarne la compatibilità ai sensi dell'art. 4 dello Statuto, o un sistema di selezione per valutarne il concreto effetto in termini di trattamento discriminatorio); ma anche di valutare, nella qui descritta prospettiva *risk-based*, quali siano i possibili e anche solo ipotetici rischi per i diritti e le libertà.

Emblematici sono in tal senso gli obblighi di trasparenza da rendere anche ai rappresentanti dei lavoratori sul funzionamento sistemi decisionali automatizzati utilizzati dalle piattaforme di lavoro. L'art. 9 della direttiva in corso di approvazione prevede l'obbligo di rendere tutta una serie dettagliata di informazioni sui sistemi decisionali e di monitoraggio automatizzati, prima della loro messa in opera o in qualsiasi momento su richiesta, anche nei confronti dei rappresentanti dei lavoratori delle piattaforme digitali; un obbligo, prima ricordato, di far partecipare e di informare i sindacati sulla "sorveglianza umana" sui sistemi automatizzati, anche tramite valutazione dell'impatto dei sistemi stessi sulle condizioni di lavoro (art. 10). Di particolare interesse è poi l'attribuzione ai rappresentanti dei lavoratori del diritto di chiedere, per conto dei lavoratori delle piattaforme, il riesame umano delle decisioni automatizzate (art. 11); così

⁽⁴⁵⁾ L. Lazzeroni, *Responsabilità sociale d'impresa 2.0. e sostenibilità digitale*, FUP, 2024.

come anche la possibilità – su specifica richiesta dei rappresentanti medesimi (v. art. 17) – di avere informazioni sul numero di persone che lavorano mediante piattaforma e sulle condizioni contrattuali applicabili; nonché la possibilità per i rappresentanti medesimi di agire, per via giudiziaria e amministrativa, per conto o a sostegno di più persone che svolgono un lavoro mediante piattaforme digitali (v. art. 19), e di poter usufruire di un canale di comunicazione con i lavoratori delle piattaforme medesime (art. 20). Si tratta di un catalogo di diritti finalizzati a un coinvolgimento dei soggetti collettivi nella comprensione dei meccanismi di funzionamento dei sistemi automatizzati abbastanza corposo, che potrebbe garantire significativi spazi di trasparenza, di coinvolgimento e di interlocuzione dei sindacati sulle modalità di funzionamento delle piattaforme di lavoro.

Così nel contesto nazionale, l'approvazione del d.lgs. n. 104 del 2022⁽⁴⁶⁾, cosiddetto Decreto trasparenza, ha segnato un deciso passo in avanti verso l'introduzione di un vero e proprio principio trasversale di trasparenza nei rapporti di lavoro che riguarda in modo significativo anche i sistemi decisionali automatizzati, in quanto il decreto stesso – introducendo l'art. 1-bis al d.lgs. 157 del 1997 – ha espressamente attribuito alle organizzazioni sindacali italiane il diritto di accedere ai dati e di richiedere le informazioni sulle modalità di funzionamento dei sistemi decisionali (oggi)⁽⁴⁷⁾ integralmente automatizzati. Il diritto di accesso, di informativa e di chiarimento della logica e del funzionamento dei sistemi automatizzati è attribuito al singolo, che può esercitarlo anche per il tramite delle rappresentanze sindacali, aziendali o territoriali, ma anche direttamente alla rappresentanza collettiva (in particolare, ai sensi del comma 6, alle rappresentanze sindacali aziendali ovvero alla rappresentanza sindacale unitaria e, in assenza delle predette rappresentanze, alle sedi territoriali delle associazioni sindacali comparativamente più rappresentative sul piano nazionale). Si tratta di uno strumento che il sindacato ha preso “molto sul serio” spingendosi, in una pluralità di casi, a dare vita a una vera e propria *strategic litigation* ⁽⁴⁸⁾ (attivata con il ricorso

⁽⁴⁶⁾ Su tale disposizione il dibattito dottrinale è ormai ampissimo, per alcuni riferimenti si rinvia a M.T. Carinci, S. Giudici, P. Perri, *Obblighi di informazione e sistemi decisionali e di monitoraggio automatizzati (art. 1-bis “Decreto Trasparenza”): quali forme di controllo per i poteri datoriali algoritmici?* *Labor*, 2023, n. 1, 7 ss.; G. Recchia, *Condizioni di lavoro trasparenti, prevedibili e giustiziabili: quando il diritto di informazione sui sistemi automatizzati diventa uno strumento di tutela collettiva*, *q. Riv.*, 2023, n. 1, 34 ss.; A. Tursi, *Trasparenza e “diritti minimi” dei lavoratori nel decreto trasparenza*, *DRI*, 2023, n. 1, 1 ss.; A. Allamprese - S. Borelli, *L'obbligo di trasparenza senza la prevedibilità del lavoro. Osservazioni sul decreto legislativo n. 104/2022*, *RGL*, 2022, n. 4, 671 ss.; L. Tebano, *I diritti di informazione nel d.lgs. n. 104/2022. Un ponte oltre la trasparenza*, *LDE*, 2024, n. 1, 1 ss.

⁽⁴⁷⁾ Com'è noto, il cosiddetto Decreto Lavoro del 2023 (D.l. 4 maggio 2023, n. 48, convertito in l. 3 luglio 2023 n. 85), nell'ottica di alleggerire gli adempimenti per le imprese, è infatti intervenuto anche sul d.lgs. n. 104 del 2022, limitando l'obbligo informativo in capo al datore ai casi in cui i sistemi in questione siano “integralmente” automatizzati. Con l'aggiunta di tale avverbio, che limita gli obblighi di informativa ai sistemi “integralmente” automatizzati, si è voluto pertanto intervenire tentando di alleggerire gli adempimenti per le imprese.

⁽⁴⁸⁾ G. Gaudio, *Algorithmic management, sindacato e tutela giurisdizionale*, *DRI*, 2022, n. 1, 30 ss.

allo strumento processuale dell'art. 28 dello Statuto) conclusasi, al momento, con tre provvedimenti di condanna⁴⁹ per le piattaforme, colpevoli di non aver reso al sindacato informazioni sufficientemente esaustive, per esempio – come si legge nel caso affrontato dal Tribunale di Palermo del 20 giugno 2023 – “sulla valutazione di impatto algoritmico” comprensiva degli schemi esecutivi relativi alle singole voci e ai parametri utilizzati, alla loro interazione e peso, ecc.; o ancora – come si legge nel caso affrontato dal Tribunale di Torino del 5 agosto 2023 – sul dove e come intervenisse il controllo umano.

I casi citati, azionati dal sindacato, dimostrano come la tenacità dell'iniziativa sindacale volta a comprendere le logiche di funzionamento dell'algoritmo, stia trasformando il principio di trasparenza, da mera regola di trasmissione delle informazioni, a un vero e proprio strumento finalizzato alla comprensione delle logiche di gestione delle risorse umane da parte dei sistemi di intelligenza artificiale, in funzione di riequilibrio dell'assetto di poteri. Una informazione che passa per la comprensione e, dunque, anche per la necessaria spiegazione, funzionale alla prevedibilità e all'apertura di spazi di controllo sull'esercizio *contra legem*, arbitrario, abusivo o discriminatorio dei poteri datoriali, ma anche all'avvio di un potenziale modello di coinvolgimento sindacale nella valutazione preventiva del rischio connesso all'utilizzo di sistemi di IA ad alto rischio. La trasparenza sulle modalità di esercizio dei poteri datoriali automatizzati, dunque, non è fine a sé stessa. Si tratta di una funzione di disvelamento sull'organizzazione di impresa che travalica il complesso mondo delle piattaforme: capire come funziona un sistema decisionale automatizzato è, infatti, funzionale ad assicurare al singolo, ma anche al sindacato, l'effettività di una serie di disposizioni tipicamente lavoristiche, ma anche di partecipare attivamente alla gestione *risk-based*.

La trasparenza, dunque, assurge anche al ruolo di veicolo di emersione dei potenziali rischi per i diritti e le libertà, anche solo disvelando il mancato rispetto di un approccio antropocentrico (la mancanza di una reale sorveglianza umana).

Tanto maggiore è la complessità dei contesti lavorativi digitalizzati, tanto più la trasparenza, la comunicazione e l'informazione divengono strumenti per creare un ambiente di fiducia, antropocentrico, per i singoli come per il sindacato, per ridurre i comportamenti opportunistici fondati sulla consapevolezza delle difficoltà che incontra il lavoratore e il soggetto collettivo per conoscere i dati gestionali, per controllarne la loro intrinseca razionalità oscurata dalla *black box*, ma anche per prevenire i rischi, quelli noti, e quelli ancora forse nemmeno immaginabili senza adeguate conoscenze su come funzioni realmente l'IA.

⁴⁹ Trib. Palermo 31 marzo 2023; Trib. Palermo 20 giugno 2023; Trib. Torino 5 agosto 2023. V. G. Recchia, *Condizioni di lavoro trasparenti, prevedibili e giustiziabili*, cit., 2023, n. 1, 34 ss.; G. Peluso, *Obbligo informativo e sistemi integralmente automatizzati*, q. Riv., 2023, n. 2, 99 ss.

7. Verso una necessaria co-progettazione della gestione del rischio

Si è detto come dal modello europeo di regolazione del digitale emerga l'idea che le previsioni e le azioni correttive umane possano influenzare i contesti con i quali i sistemi di IA interagiscono nella misura in cui la gestione del rischio sia costante e messa in atto mediante un "processo iterativo continuo eseguito nel corso dell'intero ciclo di vita di un sistema di IA ad alto rischio"⁽⁵⁰⁾. Il carattere relazionale del rischio⁽⁵¹⁾ connesso anche alla capacità informativa dell'utente o del soggetto su cui il sistema di IA impatta, alla sua esperienza, alla sua istruzione e alla sua formazione richiede approcci diversificati, tanto più necessari quanto più diversificati oggi sono anche i *workplace* attraversati dalla tecnologia, che richiedono strategie regolative sempre più adattabili e modulabili⁽⁵²⁾.

L'impatto dei sistemi di IA ad alto rischio non è univocamente generalizzabile, dovendo essere contestualizzato nell'utilizzo che ne fa il *deployer*, la piattaforma, ecc., e quindi "minimizzabile" se introdotto in un ambiente lavorativo in cui prevale una logica collaborativa e fiduciaria⁵³, oppure aggravabile a seconda del contesto relazionale o della particolare situazione di vulnerabilità di alcuni soggetti che determina o amplifica fattori di disuguaglianza oltre limiti da ritenere inaccettabili. Tutto questo la IA non lo può sapere. Lo può sapere solo l'uomo (che sia il *deployer*, il lavoratore o il sindacato).

Se il rischio va graduato in relazione a diverse situazioni di vulnerabilità e la sua mitigazione va calibrata alla luce del pericolo di effetti negativi sul target, nell'ambito dei luoghi di lavoro, solo una attività di co-progettazione⁵⁴ dei sistemi basati sull'IA con il coinvolgimento di organismi rappresentativi di interessi non solo dei lavoratori quali parti del rapporto di lavoro, ma anche e più in generale della necessaria antropocentricità dei sistemi di IA, potrebbe garantire che le innovazioni siano impiegate in modo coerente con una logica di razionalità umana e in modo da non ledere i diritti fondamentali del lavoro.

Come è stato scritto, sia le infrastrutture digitali, sia le reti di comunicazione, sia gli istituti giuridici si trovano a metà tra verità e potere⁵⁵ e hanno carattere ambivalente: possono cioè essere sia mezzi di emancipazione, sia incubatori di pratiche di potere; la loro ambivalenza risiede appunto nella loro capacità di autorizzare, trasmettere e modulare flussi informativi e schemi comportamentali di fatto "mediando" tra verità e

⁽⁵⁰⁾ Art. 9, par. 2, IA Act.

⁽⁵¹⁾ M. Catanzariti, *Rischio e vulnerabilità nel modello europeo di intelligenza artificiale*, cit., 75.

⁽⁵²⁾ B. Caruso - L. Zappalà, *Un diritto del lavoro "tridimensionale": valori e tecniche di fronte ai mutamenti dei luoghi di lavoro*, in R. Del Punta (a cura di), *Valori e tecniche nel diritto del lavoro*, FUP, 2022, 23 ss.

⁽⁵³⁾ B. Caruso, *Impresa partecipata e contratto di lavoro*, cit., 1 ss.

⁽⁵⁴⁾ A. Aloisi - V. De Stefano, *Between risk mitigation and labour rights enforcement*, cit., 307.

⁽⁵⁵⁾ J. Cohen, *Between Truth and Power: The Legal Constructions of Information Capitalism*, Oxford, 2019, 5 ss.

potere. Il sindacato è aduso a tale mediazione, tanto più necessaria quanto più la verità di cui si discute nelle pagine del presente scritto non è una verità nemmeno effettivamente reale, ma solo quella creata da algoritmi, inferenziale, frutto di un computo non umano, fondata su dati non sempre verificabili. I rischi che questa verità artificiale si trasformi e supporti i poteri datoriali sono sempre più elevati, ragione per cui spingere il sindacato a anticipare la propria mediazione *ex ante* e in via precauzionale sul rischio non significa abbandonare l'approccio *rights-based*, significa piuttosto provare a introitare a monte del processo di gestione dei rischi i valori: quelli della persona, dei suoi diritti e delle sue libertà.

Bibliografia

- Alaimo A., *I nuovi termini del discorso giuridico sulla partecipazione dei lavoratori. Partecipazione organizzativa e diretta versus partecipazione indiretta: per una dialettica senza contrapposizione*, in WP CSDLE “Massimo D’Antona”.IT – 480/2024.
- Alemanno A., *Regulating the European Risk Society*, in A. Alemanno - F. Den Butter - A. Nijsen - J. Torriti (a cura di), *Better Business Regulation in a Risk Society*, Springer, 2012, 37 ss.
- Allamprese A. - Borelli S., *L’obbligo di trasparenza senza la prevedibilità del lavoro. Osservazioni sul decreto legislativo n. 104/2022*, in RGL, 2022, n. 4, 671 ss.
- Aloisi A. - De Stefano V., *Between risk mitigation and labour rights enforcement: Assessing the transatlantic race to govern AI-driven decision-making through a comparative lens*, in ELLJ, 2023, n. 2, 283 ss.
- Barbera M., *“La nave deve navigare”. Rischio e responsabilità al tempo dell’impresa digitale*, in LLI, 2023, n. 2, 3 ss.
- Beck U., *Risk Society: Towards a New Modernity*, Sage, 1992.
- Borelli S. - Brino V. - Faleri C. - Lazzeroni L. - Tebano L. - Zappalà L., *Lavoro e tecnologie*, Giappichelli, 2020.
- Brino V., *La governance societaria sostenibile: un cantiere da esplorare per il diritto del lavoro?* in LD, 2023, n. 3, 445 ss.
- Carinci M.T., Giudici S., Perri P., *Obblighi di informazione e sistemi decisionali e di monitoraggio automatizzati (art. 1-bis “Decreto Trasparenza”): quali forme di controllo per i poteri datoriali algoritmici?* in Labor, 2023, n. 1, 7 ss.
- Carrieri M. – Pirro F., *Digitalizzazione, relazioni industriali e sindacato. Non solo problemi, ma anche opportunità*, in A. Cipriani - A. Grimolati - G. Mari (a cura di), *Il lavoro 4.0. La quarta rivoluzione industriale e le trasformazioni delle attività lavorative*, Firenze, 2018, 131 ss.
- Caruso B. – Zappalà L., *Un diritto del lavoro “tridimensionale”: valori e tecniche di fronte ai mutamenti dei luoghi di lavoro*, in R. Del Punta (a cura di), *Valori e tecniche nel diritto del lavoro*, FUP, 2022, 23 ss.
- Caruso B., Del Punta R., Treu T., *Manifesto per un diritto del lavoro sostenibile*, in CSDLE “Massimo D’Antona”, 2020, 53 ss.
- Caruso B., *Il sindacato tra funzioni e valori nella “grande trasformazione”. L’innovazione sociale in sei tappe*, in B. Caruso - R. Del Punta - T. Treu (a cura di), *Il diritto del lavoro e la grande trasformazione*, il Mulino, 2020, 145 ss.
- Caruso B., *Impresa partecipata e contratto di lavoro*, in WP CSDLE “Massimo D’Antona”.IT – 484/2024.
- Catanzariti M., *Rischio e vulnerabilità nel modello europeo di intelligenza artificiale*, in SocietàMutamentoPolitica, 2022, n. 13, 73 ss.
- Chiaromonte W., *Lavoro (povero) tramite piattaforme digitali, rappresentanza e tutela collettiva fra sindacalismo informale e sindacalismo tradizionale*, in L. Chies - M.D. Ferrara - E. Podrecca (a cura di), *Le dimensioni della povertà*, Giappichelli, 2021, 263 ss.
- Cohen J., *Between Truth and Power: The Legal Constructions of Information Capitalism*, Oxford, 2019, 5 ss.
- De Gregorio G. – Dunn P., *The European Risk-Based approaches: Connecting Constitutional Dots in The Digital age*, in *Common Market Law Review*, 2022, 473 ss.
- De Gregorio G., *The rise of digital constitutionalism in the European Union*, in *International Journal of Constitutional Law*, 2021, n. 1, 41 ss.
- Del Punta R., *I diritti fondamentali e la trasformazione del diritto del lavoro*, in WP CSDLE “Massimo D’Antona”.IT – 333/2017.
- Del Punta R., *Un diritto del lavoro 4.0*, in A. Cipriani - A. Grimolati - G. Mari (a cura di), *Il lavoro 4.0. La quarta rivoluzione industriale e le trasformazioni delle attività lavorative*, FUP, 2018, 224 ss.
- Faleri C., *Brevi spunti di riflessione sull’evoluzione delle relazioni sindacali nell’economia digitale*, in *Ianus DF*, 2021, n. 24, 93 ss.
- Faleri C., *Diritti di informazione e principio di trasparenza per una governance societaria sostenibile*, in LD, 2023, n. 3, 545 ss.
- Finocchiaro G., *La proposta di Regolamento sull’intelligenza artificiale: il modello europeo basato sulla gestione del rischio*, in *Il diritto dell’informazione e dell’informatica*, 2022, n. 2, 303 ss.

- Floridi L., *Establishing the Rules for Building Trustworthy AI*, *Nature Machine Intelligence*, 2019, 261 ss.
- Forlivesi M., *Interessi collettivi e rappresentanza dei lavoratori del web*, in P. Tullini (a cura di), *Web e lavoro. Profili evolutivi e di tutela*, Giappichelli, 2017, 192 ss.
- Gaudio G., *Algorithmic management, sindacato e tutela giurisdizionale*, in *DRI*, 2022, n. 1, 30 ss.
- Gellert R., *The Risk-Based Approach to Data Protection*, Oxford, 2020.
- Imberti L., *Intelligenza artificiale e sindacato. Chi controlla i controllori artificiali?* in *federalismi.it*, 2023, n. 29, 192 ss.
- Ingrao A., *Il controllo a distanza sui lavoratori e la nuova disciplina privacy. Una lettura integrata*, Cacucci, 2018, 133 ss.
- Lamannis M., *Collective bargaining in the platform economy: a mapping exercise of existing initiatives*, ETUI, 2023.
- Lassandari A., *La tutela collettiva del lavoro nelle piattaforme digitali: gli inizi di un percorso difficile*, in *LLI*, 2018, n. 1, IV ss.
- Lazzeroni L., *Responsabilità sociale d'impresa 2.0. e sostenibilità digitale*, Firenze, 2024.
- Loi P., *Il rischio proporzionato nella proposta di regolamento sull'IA e i suoi effetti nel rapporto di lavoro*, in *federalismi.it*, 2023, n. 4, 239 ss.
- Loi P., *Rischio e sicurezza nel rapporto di lavoro*, in *RGL*, 2013, n.3, 569 ss.
- Lupton D., *Digital risk society*, in A. Burgess - A. Alemanno - J. Zinn (a cura di), *Routledge Handbook of Risk Studies*, London, 2016, 301 ss.
- Macenaite M., *The "Riskification" of European Data Protection Law through a two-fold Shift*, *European Journal of Risk Regulation*, 2017, n. 3, 506 ss.
- Magnani M., *Nuove tecnologie e diritti sindacali*, in *LLI*, 2019, n. 2, 3 ss.
- Mahler T., *Between Risk Management and Proportionality: The Risk-based Approach in the EU's Artificial Intelligence Act Proposal*, *Nordic Yearbook of Law and Informatics*, 2021, 258 ss.
- Miranda Boto J.M- Brameshuber E. - Loi P. - Ratti L. (a cura di), *Contrattazione Collettiva e gig economy. Uno strumento tradizionale per nuovi modelli di organizzazione*, Torino, 2022.
- OECD *Employment Outlook 2023: Artificial Intelligence and the Labour Market*, OECD Publishing, 2023.
- Peluso G., *Obbligo informativo e sistemi integralmente automatizzati*, in *LLI*, 2023, n. 2, 99 ss.
- Peruzzi M., *Il dialogo sociale di fronte alle sfide della digitalizzazione*, in *DRI*, 2020, 1213 ss.
- Peruzzi M., *Intelligenza artificiale e lavoro*, Giappichelli, 2023, 37 ss.
- Peruzzi M., *Intelligenza artificiale e lavoro: l'impatto dell'AI Act nella ricostruzione del sistema regolativo Ue di tutela*, in M. Biasi (a cura di), *Diritto del lavoro e intelligenza artificiale*, Giappichelli, 2024, 115 ss.
- Pigni G., *European Social Partners Framework Agreement on digitalisation: ottimizzare i benefici ed affrontare insieme le sfide della digitalizzazione*, BA, 2020, n. 26.
- Prassl J., *Collective Voice in the Platform Economy: Challenges, Opportunities, Solution*, Report to the ETUC, 2018.
- Purificato I., *Governare l'innovazione tecnologica: il rilancio del metodo partecipativo in rapporto sinergico con la contrattazione collettiva*, in *Quaderno della Rivista Diritti Lavori Mercati*, 2023, 121 ss.
- Recchia G., *Alone in the crowd? La rappresentanza e l'azione collettiva ai tempi della Sharing Economy*, in *RGL*, 2018, n. 1, 144 ss.
- Recchia G., *Condizioni di lavoro trasparenti, prevedibili e giustiziabili: quando il diritto di informazione sui sistemi automatizzati diventa uno strumento di tutela collettiva*, in *LLI*, 2023, n. 1, 34 ss.
- Rota A., *Sull'Accordo quadro europeo in tema di digitalizzazione del lavoro*, in *LLI*, 2020, n. 2, 25 ss.
- Tebano L., *I diritti di informazione nel d.lgs. n. 104/2022. Un ponte oltre la trasparenza*, in *LDE*, 2024, n. 1, 1 ss.
- Treu T., *La digitalizzazione del lavoro: proposte europee e piste di ricerca*, in *federalismi.it*, 2022, n. 9, 190 ss.
- Tullini P., *L'economia digitale alla prova dell'interesse collettivo*, in *LLI*, 2018, n. 1, 4 ss.
- Tursi A., *Trasparenza e "diritti minimi" dei lavoratori nel decreto trasparenza*, in *DRI*, 2023, n. 1, 1 ss.
- Van Dijk N. - Gellert R. - Rommetveit K., *A risk to a right? Beyond data protection risk assessments*, *Computer Law & Security Review*, 2016, n. 2, 286 ss.
- Zappalà L., *Transparency and comprehensibility of working conditions and automated decisions: is it possible to open the black box?* in *The Italian Law Journal*, 2023, n. 2.
- Zappalà L., *Vulnerabili digitali, poveri della rete e padroni del tempo: l'approccio rimediale case-by-case nel lavoro delle piattaforme*, in B. Caruso (a cura di), *Il lavoro povero sans phrase*, il Mulino, 2024, 283 ss.
- Zoppoli L., *La partecipazione sindacale nella civiltà digitale*, in *DRI*, 2023, 958 ss.