Fondazione Marco Biagi

UNIMORE
UNIVERSITÀ DEGLI STUDI DI MODENA E REGGIO EMILIA

QUADERNI FONDAZIONE MARCO BIAGI

Lavoro, Impresa e Nuove Tecnologie dopo l'AI Act

Simone Scagliarini, Iacopo Senatori (a cura di)

2024

Quaderni Fondazione Marco Biagi

ISSN 2239-6985
Registrazione presso il Tribunale di Modena n. 2031 del 03/05/2011

Lavoro, Impresa e Nuove Tecnologie dopo l'AI Act
Simone Scagliarini, Iacopo Senatori (a cura di). Modena: Fondazione Marco Biagi, 2024

ISBN 979-12-81397-16-3

Editore
Fondazione Marco Biagi, Università di Modena e Reggio Emilia
Largo Marco Biagi 10, 41121 Modena
Tel. +39 059 2056031
E-mail: fondazionemarcobiagi@unimore.it

INDICE

PRESENTAZIONE

Questo Volume raccoglie, ampliati e arricchiti, alcuni dei contributi presentati nell'incontro di studi *Lavoro, Impresa e nuove tecnologie dopo l'AI Act*, organizzato dalla Fondazione Marco Biagi dell'Università di Modena e Reggio Emilia il 14 maggio 2024, per avviare un dialogo intorno al Regolamento europeo sull'intelligenza artificiale[1], analizzandone criticamente, a prima lettura, alcune tra le disposizioni più significative per le conseguenze sulla *governance* aziendale e la gestione dei rapporti di lavoro.

L'atto normativo in questione, all'epoca, attendeva ancora l'approvazione definitiva da parte del Consiglio UE, avvenuta poi il 21 maggio 2024. Il procedimento si è poi perfezionato con la pubblicazione nella Gazzetta Ufficiale dell'UE il 12 luglio 2024, quando questo Volume era in lavorazione.

La portata rivoluzionaria del Regolamento, che ne fa una novità dirompente nel panorama normativo globale per quanto riguarda l'impatto della transizione tecnologica sui diritti delle persone e sulle relazioni sociali ed economiche, incluse quelle di lavoro, giustifica tuttavia ampiamente il grande interesse che esso ha suscitato, tanto in dottrina quanto nella pubblica opinione, già durante tutte le fasi del suo non brevissimo *iter*, e spiega le ragioni per cui anche la Fondazione Marco Biagi ha sentito l'esigenza di non sottrarsi ad un coinvolgimento in questo attualissimo dibattito che, comprensibilmente, appare già ricco e non privo di fondamentali apporti critici.

Del resto, da anni la Fondazione, attraverso i suoi *Osservatori*, ha posto il tema della trasformazione digitale del lavoro, dell'impresa e, più in generale, dell'economia al centro della propria elaborazione scientifica e culturale, accompagnandone i progressivi sviluppi con iniziative di ricerca, formazione e "terza missione" universitaria. Non poteva, dunque, che essere colta tempestivamente anche l'occasione di avviare l'analisi e la riflessione sui contenuti innovativi del Regolamento e sul suo impatto sistematico, in un ordinamento che viene via via assumendo, su questa materia, una crescente complessità per effetto del susseguirsi di interventi normativi di matrice europea, che peraltro hanno da sempre costituito il fulcro dell'attenzione dello Studioso la cui eredità scientifica la Fondazione intende promuovere.

Peraltro, detti interventi presentano per molti versi un oggetto affine, se non sovrapposto,

[1] Regolamento (UE) 2024/1689 del Parlamento Europeo e del Consiglio, in GU L 144 del 12 luglio 2024.

andando a regolare ambiti contigui, quando non coincidenti, volta per volta sotto una prospettiva diversa, ciò che ulteriormente rimarca ed accresce la complessità del sistema. Si pensi, per limitarci ad un solo, ma paradigmatico, esempio, alla questione del *management* algoritmico, su cui insistono fonti diverse come il GDPR, l'*AI Act* e la recentissima Direttiva sul lavoro tramite piattaforma digitale.

Da tali spunti è scaturito, per iniziativa degli Osservatori *Lavoro digitale e multilocale* e *Privacy, intelligenza artificiale e nuove tecnologie*, l'incontro di studi di cui questo Volume restituisce i risultati.

In coerenza con la radicata impostazione metodologica della Fondazione, i contributi raccolti nel Volume affrontano il tema da molteplici prospettive disciplinari: segnatamente, quelle del diritto costituzionale, del diritto del lavoro e del diritto privato. Fa, poi, un particolare piacere segnalare come tra gli autori figurino, insieme a studiosi di consolidata esperienza, giovani assegniste e dottoresse di ricerca formatesi nel dottorato in *Lavoro, Sviluppo e Innovazione*, istituito presso il Dipartimento di Economia "Marco Biagi" dell'Università di Modena e Reggio Emilia in collaborazione con la Fondazione Marco Biagi: a conferma dell'impegno dell'Università e della Fondazione stesse nella crescita di una nuova generazione di studiosi e studiose attrezzati ad affrontare con metodo scientifico ed approccio critico le sfide contemporanee.

Modena, 18 luglio 2024

Simone Scagliarini
Iacopo Senatori

INTRODUZIONE. L'AI ACT: UN NUOVO TASSELLO NELLA COSTRUZIONE DELL'ORDINAMENTO DEL LAVORO DIGITALE

Iacopo Senatori
Associato di Diritto del lavoro nell'Università degli studi di Modena e Reggio Emilia

L'applicazione di tecnologie di automazione e "abilitanti" nei contesti produttivi si riflette sugli interessi dei lavoratori da due prospettive: quella gestionale, rispetto alla quale rilevano gli effetti potenziali della sostituzione dell'uomo da parte delle macchine nell'esercizio delle funzioni organizzative e decisionali d'impresa che impattano sulle dinamiche del rapporto di lavoro, e quella di mercato, che guarda alle ripercussioni della trasformazione tecnologica sui livelli occupazionali e sulla professionalità dei lavoratori, stretta tra obsolescenza e necessità di rinnovamento[2].

Se l'intelligenza artificiale (IA) rappresenta, ad oggi, lo stadio più progredito del fenomeno appena descritto[3], in queste brevi note, dedicate a tratteggiare gli spunti di analisi posti dal nuovo Regolamento europeo noto come *AI Act*, vorrei concentrarmi sul primo dei profili indicati: quello dell'impatto delle tecnologie sui poteri datoriali, e, di conseguenza, dell'effettività delle garanzie previste dall'ordinamento a favore dei lavoratori verso i quali detti poteri sono esercitati.

Me ne occuperò in termini generali, dal momento che i contributi che seguono in questo Volume li affronteranno in maggiore dettaglio.

Il filo conduttore che intendo seguire è quello delle tecniche di tutela: materia rispetto alla quale il diritto del lavoro sta sperimentando un'evoluzione. Sempre più, infatti, alla tecnica classica, di tipo prescrittivo-rimediale, basata sulla norma inderogabile e sullo schema obbligo/sanzione, si affiancano tecniche di matrice preventiva e promozionale, che impongono l'adozione di procedure mirate al conseguimento di un risultato (ad esempio, la garanzia della parità retributiva tra uomini e donne)[4] o evitare il verificarsi di un evento o di un pregiudizio ai danni di un individuo, con una espansione di un approccio tipico di alcuni settori dell'ordinamento come quello della sicurezza sul lavoro e della *privacy*.

---

[2] Cfr. BORELLI S., BRINO V., FALERI C., LAZZERONI L., TEBANO L., ZAPPALÀ L., *Lavoro e tecnologie. Dizionario del diritto del lavoro che cambia*, Giappichelli, Torino, 2022, ma già FAIOLI M., *Mansioni e macchina intelligente*, Giappichelli, Torino, 2018.

[3] PONCE DEL CASTILLO A., *AI: the value of precaution and the need for human control*, in PONCE DEL CASTILLO A. (ed.), *Artificial intelligence, labour and society*, ETUI Printshops, Brussels, 2024, 13 ss.

[4] Cfr. la Direttiva (UE) 2023/970 del Parlamento europeo e del Consiglio del 10 maggio 2023 volta a rafforzare l'applicazione del principio della parità di retribuzione tra uomini e donne per uno stesso lavoro o per un lavoro di pari valore attraverso la trasparenza retributiva e i relativi meccanismi di applicazione, in GU L 132 del 17.5.2023.

Quest'ultimo è un approccio che va affermandosi anche nell'ambito della regolazione dell'uso delle nuove tecnologie, sul lavoro e non solo[5]. Ne costituisce un esempio palese proprio l'*AI Act*, con la sua impostazione metodologica *risk-based*, della quale molto si dirà nei contributi che seguono. Tale impostazione, che ordina i rischi legati all'uso dell'intelligenza artificiale lungo una struttura piramidale, ha carattere sostanzialmente permissivo: fatta eccezione dei rischi che il Regolamento assume come inaccettabili, e che determinano il divieto di uso dell'IA (parliamo ad esempio delle pratiche manipolative della volontà delle persone, di *social rating*, di predizione della commissione di reati), la scelta del legislatore è quella di consentire l'immissione sul mercato dei sistemi di intelligenza artificiale, condizionandola all'adozione di cautele che consentano di eliminare o ridurre i rischi, possibilmente già nella fase di progettazione del sistema, oppure di mitigare l'impatto del rischio, laddove questo non sia eliminabile in fase di progettazione.

Siffatto metodo regolativo pone due questioni, nella prospettiva del rapporto di lavoro: la prima, in che misura si può accettare un rischio immanente o ineliminabile quando sono coinvolti i diritti fondamentali; la seconda, se la tecnica procedurale/preventiva adottata dall'*AI Act*, per come si configura, tenga in adeguata considerazione le specifiche caratteristiche del rapporto di lavoro.

Prima di approfondire questi due quesiti è utile riassumere, molto brevemente, quali connotati assuma la trasformazione dei poteri datoriali per effetto delle nuove tecnologie.

La letteratura giuslavoristica ha iniziato da tempo a censire i dispositivi di nuova generazione utilizzati dalle imprese nella gestione dell'organizzazione del lavoro, anche sotto il profilo dell'impatto che esercitano sulla sfera dell'adempimento dell'obbligazione lavorativa. Espressioni come "Human Resource Management algoritmico" e "People Analytics" richiamano una funzione gestionale che fa leva su tecnologie dette "abilitanti" per consentire al datore di lavoro di massimizzare l'efficienza e ridurre i costi dei processi decisionali incidenti su tutte le fasi del rapporto di lavoro: dalla selezione e reclutamento all'organizzazione degli orari, alla valutazione dei fabbisogni formativi, alla valutazione del rendimento e così via[6].

In forza di queste tecnologie abilitanti, il potere datoriale si accentua in tre direzioni[7]:

[5] Coglie questa tendenza PERUZZI M., *Intelligenza artificiale e lavoro. Uno studio su poteri datoriali e tecniche di tutela*, Giappichelli, Torino, 2023.
[6] Cfr. GAUDIO G., Algorithmic management, *poteri datoriali e oneri della prova: alla ricerca della verità materiale che si cela dietro l'algoritmo*, in *Labour & Law Issues*, 2020, 6(2), 19; DAGNINO E., People Analytics*: lavoro e tutele al tempo del management tramite* big data, in *Labour & Law Issues*, 2020, 3(1), 1.
[7] Cfr. ADAMS-PRASSL J., *The Challenges of Management by Algorithm: Exploring Individual and Collective Aspects*, in GYULAVÀRI T., MENEGATTI E. (eds.), *Decent Work in the Digital Age. European and Comparative Perspectives*, Hart, London, 2022, 231.

- il potere diventa "mediato", rispetto al fattore umano, poiché sovente il *manager* non dispone di un effettivo margine di intervento sull'elaborazione dei dati che conduce ad una certa decisione, per cui non può modificarla ma solo recepirla, quando non sia estromesso del tutto dal processo decisionale;
- il potere diventa "aumentato", perché cresce la sua capacità di coprire la sfera della prestazione lavorativa sia in ampiezza (per esempio ricostruendo dai dati biometrici informazioni sugli stati d'animo dei lavoratori, quali stanchezza, irritazione e così via) sia in profondità (ad es. monitorando il numero e la qualità delle operazioni compiute in unità infinitesimali di tempo)[8];
- il potere diventa, soprattutto, opaco, perché si perviene alla decisione attraverso un sistema di elaborazione dei dati alla cui base stanno formule matematiche e moli di dati sostanzialmente non intellegibili, spesso perfino per il datore di lavoro. In altre parole: non è sempre chiaro quali dati si estraggono, in base a quali parametri vengono trattati e attraverso quali passaggi si determina la decisione, e con quale rapporto di causa-effetto.

Il potere si fa quindi più pervasivo, essendo in grado di raggiungere sfere di intimità personale del lavoratore prima inaccessibili. Nel contempo, diminuisce la possibilità di esercitare un controllo sull'esercizio del potere, al prezzo di indebolire la capacità di reazione dei lavoratori a forme di esercizio che determinino una lesione illegittima dei loro diritti. Paradigmatico è il caso delle discriminazioni, dirette ma ancor più indirette, poiché il datore, per difendere la legittimità di una certa decisione, potrebbe semplicemente imputare alla "scatola nera" dell'algoritmo, da un lato, l'elaborazione delle informazioni che hanno determinato la decisione, e dall'altro la valutazione circa la proporzionalità tra mezzi e fini che ha informato la decisione, spogliandosi di qualsiasi responsabilità e precludendo al giudice di ricostruire il processo deliberativo per poterne sindacare la legittimità[9].

Poste queste premesse, per poter rispondere ai due quesiti formulati dinanzi occorre ricostruire i profili dell'*AI Act* che presentano una specifica connotazione lavoristica.

Prendendo le mosse dalla tecnica di tutela che ho definito classica, quella fondata sul binomio prescrizione (di obbligo o divieto) - sanzione, sono relativamente pochi i divieti di pratiche di IA elencati nel Regolamento che abbiano una diretta applicazione lavoristica. Il

[8] Cfr. ALOISI A., *Automation, Augmentation, Autonomy: Labour Regulation and the Transformation of Managerial Prerogatives*, in GYULAVÀRI T., MENEGATTI E. (eds.), *Decent Work in the Digital Age. European and Comparative Perspectives*, Hart, London, 2022, 245.

[9] Cfr., da ultima, TOPO A., *Nuove tecnologie e discriminazioni*, Relazione al XXI Congresso nazionale AIDLaSS *Diritto antidiscriminatorio e trasformazioni del lavoro*, Messina, 23-25 maggio 2024, https://aidlass.it/le-relazioni-del-xxi-congresso-nazionale-messina-2024/ (consultato il 23 giugno 2024).

riferimento è al divieto di immissione sul mercato, messa in servizio o uso di sistemi di IA per inferire le emozioni di una persona fisica nell'ambito del luogo di lavoro e degli istituti di istruzione, tranne laddove l'uso del sistema di IA sia destinato a essere messo in funzione o immesso sul mercato per motivi medici o di sicurezza; e del divieto di immissione sul mercato, messa in servizio o uso di sistemi di categorizzazione biometrica che classificano individualmente le persone fisiche sulla base dei loro dati biometrici per trarre deduzioni o inferenze in merito a razza, opinioni politiche, appartenenza sindacale, convinzioni religiose o filosofiche, vita sessuale o orientamento sessuale.

Per il resto occorre fare riferimento al livello intermedio della piramide, quello del "rischio elevato". Ciò che ricaviamo dall'Allegato III dell'*AI Act*, che elenca i sistemi ad alto rischio, è che ricadono in tale categoria pressoché tutte le applicazioni dell'IA al rapporto di lavoro. Il punto 4 parla infatti di "Occupazione, gestione dei lavoratori e accesso al lavoro autonomo", enumerando nel dettaglio: 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. L'allegato cita inoltre i sistemi usati nella formazione e valutazione degli apprendimenti, anch'essi suscettibili di implicazioni "lavoristiche".

La logica seguita per la regolazione dei sistemi ad alto rischio è quella della prevenzione (dove il rischio è quello della violazione di un diritto fondamentale), o, qualora il rischio sia ineliminabile, della sua mitigazione. La tecnica è invece quella della imposizione di una serie di obblighi procedurali, il cui corretto assolvimento dovrebbe liberare da responsabilità nel caso in cui si verifichi un evento pregiudizievole.

Tale impianto presenta alcuni profili critici in chiave giuslavoristica, che qui possono essere riassunti solo per cenni.

Il primo è che gli obblighi gravano in misura preponderante sui fornitori (cioè sui soggetti che hanno progettato e venduto il sistema), e molto meno sui *deployer*, categoria alla quale saranno ascrivibili, nella maggioranza dei casi, i datori di lavoro[10].

I fornitori, ai sensi dell'art. 9 del Regolamento, devono porre in funzione un sistema di

[10] Di "marginalizzazione" della figura del *deployer* parla PERUZZI M., *op. cit.*, 36.

gestione dei rischi, da rivalutare e aggiornare periodicamente. Peraltro, la norma prevede un significativo ridimensionamento della portata dell'obbligo *de quo* dal momento in cui, per un verso, limita il perimetro del sistema di gestione ai rischi derivanti da un uso improprio "ragionevolmente prevedibile" e pur sempre emergente solo quando il sistema di IA sia utilizzato in conformità alla sua "finalità prevista"[11]; e, per altro verso, stabilisce che "i rischi di cui al presente articolo riguardano solo quelli che possono essere ragionevolmente attenuati o eliminati attraverso lo sviluppo o la progettazione del sistema di IA ad alto rischio o la fornitura di informazioni tecniche adeguate", mentre "le misure di gestione dei rischi di cui al paragrafo 2, lettera d), sono tali che i pertinenti rischi residui associati a ciascun pericolo nonché il rischio residuo complessivo dei sistemi di IA ad alto rischio sono considerati accettabili"[12].

Inoltre, i fornitori devono provvedere ad un adeguato addestramento dei sistemi di IA, garantendo la completezza e l'accuratezza dei dati utilizzati nonché la corretta *governance* degli stessi, e devono fornire istruzioni complete e intellegibili ai *deployer* rispetto all'uso dei sistemi.

È, tuttavia, come si accennava dinanzi, principalmente la posizione dei *deployer* rispetto agli obblighi previsti dal Regolamento a lasciare perplessi.

Infatti, gli obblighi dei *deployer* si sostanziano, in definitiva, nel seguire correttamente le istruzioni impartite dal fornitore, monitorare l'utilizzo e segnalare eventuali malfunzionamenti.

Vero è che sui *deployer* incombe anche l'obbligo di garantire la sorveglianza umana sui sistemi di IA. Questo è un aspetto positivo e qualificante dell'approccio "antropocentrico" all'IA professato dal legislatore euro-unitario. Stabilire che la sorveglianza debba essere attuata dal *deployer*, a meno che non sia già stata integrata nel sistema in fase di progettazione, costituisce infatti un primo profilo di responsabilizzazione della figura datoriale, che si sostanzia soprattutto nell'obbligo di individuare un addetto professionalmente qualificato allo svolgimento del ruolo di sorvegliante (art. 26, c. 2: "i deployer affidano la sorveglianza umana a persone fisiche che dispongono della competenza, della formazione e dell'autorità necessarie nonché del sostegno necessario"). L'addetto deve infatti poter comprendere il funzionamento del sistema, interpretarne l'output e individuarne malfunzionamenti.

[11]Giudicano tali limitazioni eccessivamente restrittive, a fronte dell'indeterminatezza delle potenziali conseguenze dannose di un uso anomalo dell'IA, che potrebbe avere un impatto sui rapporti di lavoro anche al di fuori della "finalità prevista" in fase di progettazione, CEFALIELLO A., KULLMANN M., *Offering false security: How the draft artificial intelligence act undermines fundamental workers rights*, in *European Labour Law Journal*, 2022, 13(4), 542 ss., e PONCE DEL CASTILLO A., op. cit.

[12] Il che solleva naturalmente il quesito se si debba dedurre che l'evento causato da un fattore di rischio accettabile non sia imputabile a responsabilità di alcuno e quindi non sia "giustiziabile".

E' importante sottolineare, inoltre, che l'addetto alla sorveglianza deve essere provvisto dell'autorità di decidere, in qualsiasi situazione particolare, di non usare il sistema di IA ad alto rischio o altrimenti di ignorare, annullare o ribaltare l'*output* del sistema stesso.

Il Regolamento, quindi, prevede la concreta possibilità di decisioni organizzative non totalmente subalterne all'algoritmo. C'è però da dire che, nell'impianto complessivo della norma, il processo di sorveglianza umana segue sempre una logica unilaterale e *top-down*: nulla si dice, infatti, rispetto alla possibilità dei lavoratori o dei loro rappresentanti di influenzarlo, ad esempio facendo segnalazioni[13], o di partecipare alla gestione del processo. Il controllo, quindi, esiste ma non entra nella dinamica contrattuale di amministrazione del rapporto di lavoro.

Infine, l'art. 26, comma 7, si prevede che i datori di lavoro "informano i rappresentanti dei lavoratori e i lavoratori interessati che saranno soggetti all'uso del sistema di IA ad alto rischio. Tali informazioni sono fornite, se del caso, 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".

Quello dell'informazione, soprattutto verso i soggetti collettivi, è forse, in una prospettiva lavoristica, l'aspetto più qualificante dell'intero impianto normativo. Occorre tuttavia una puntualizzazione riguardo alle diverse funzioni assolte dai diritti di informazione nell'ordinamento.

L'informazione può, prima di tutto, essere uno strumento di controllo sull'esercizio del potere. Tale è la logica applicata nel "decreto trasparenza", che ha inserito nel d. lgs. n. 152/97 l'art. 1-*bis*, dedicato proprio all'informazione da rendere in caso di utilizzo di sistemi decisionali e di monitoraggio automatizzati. Questo adempimento, se fornisce ai lavoratori gli strumenti di conoscenza necessari a rivendicare i propri diritti laddove questi siano violati per mezzo di sistemi di gestione automatizzati, non modifica però gli equilibri di potere tra la parti del rapporto di lavoro. Certo, l'informazione deve essere resa con modalità, contenuti e tempistiche adeguate, e quindi, ad esempio, prima che si inizi ad utilizzare il sistema. Ciò tuttavia non vale a mettere in discussione la scelta compiuta a monte, relativa all'uso dell'IA, e la relativa titolarità, di esclusiva spettanza del datore di lavoro.

A modificare gli equilibri di potere contribuiscono, invece, i diritti di informazione intesi come strumenti di coinvolgimento nella gestione dell'impresa, ovvero come fase propedeutica alla consultazione dei lavoratori o dei loro rappresentanti. I diritti di

[13] Eccetto che con riferimento a singole decisioni, in base all'art. 86, sul quale ritornerò; o alla possibilità, offerta dal Regolamento, di segnalare violazioni "sistemiche", ma non al datore di lavoro bensì alle autorità di vigilanza.

informazione e consultazione, disciplinati da numerose direttive europee e sanciti a livello "costituzionale" dall'art. 27 della Carta dei diritti fondamentali dell'UE, si pongono l'obiettivo di consentire ai lavoratori di esercitare un'influenza sulla successiva decisione datoriale (*an* e *quomodo*) e, pur non sussistendo un obbligo formale in tal senso, di sottoporla ad un negoziato laddove i rapporti di forza lo consentano. Questa è la direzione indicata dalle parti sociali europee nel 2020 con l'Accordo quadro sulla digitalizzazione. Un accordo che delinea un sistema di gestione della trasformazione tecnologica basato su alcuni obiettivi irrinunciabili, per esempio il controllo umano sugli algoritmi, e su un metodo di "partenariato circolare" che innerva tutte le fasi di adozione e uso delle tecnologie, inclusa l'AI, fino al punto di configurare un sistema di "contrattazione continua" avente l'obiettivo di tutelare dai rischi connessi alle tecnologie, cogliendone invece le opportunità[14].

Si tratta di un aspetto cruciale, ben evidenziato da ampi settori della dottrina giuslavoristica, che rilevano come la partecipazione effettiva dei sindacati e dei rappresentanti dei lavoratori alla *governance* dei processi di lavoro interessati dall'uso dell'intelligenza artificiale, fin dalla fase di progettazione dei sistemi, sia un fattore essenziale non solo in chiave di tutela dei lavoratori, poiché consente ad essi di esercitare un ruolo attivo di governo della trasformazione digitale senza doversi relegare ad azioni puramente difensive da attuarsi a valle della lesione di un diritto, ma anche nell'interesse aziendale al miglioramento dell'efficienza dei processi, stante il contributo che i lavoratori possono arrecare a tal fine, alla luce della loro conoscenza della realtà organizzativa[15].

Su tale aspetto si rileva un vizio prospettico dell'*AI Act*. Il considerando 92 infatti, dopo aver precisato (ma ce n'era bisogno?) che il Regolamento non pregiudica i diritti di informazione e consultazione dei lavoratori previsti nel diritto UE, afferma che "rimane necessario garantire che i lavoratori e i loro rappresentanti siano informati in merito alla diffusione programmata dei sistemi di IA ad alto rischio sul luogo di lavoro, qualora non siano soddisfatte le condizioni per tali obblighi di informazione o di informazione e consultazione previsti da altri strumenti giuridici"[16]. Inoltre, tale diritto di informazione è accessorio e necessario rispetto all'obiettivo di tutelare i diritti fondamentali alla base del presente regolamento. È pertanto opportuno prevedere nel presente regolamento un obbligo

[14] Sul punto sia consentito il rinvio a SENATORI I., *The European Framework Agreement on Digitalisation: a Whiter Shade of Pale?*, in *Italian Labour Law E-Journal*, 2020, 13(2), 159.
[15] Cfr. *ex multis* KLENGEL E., WENCKEBACH J., *Artificial intelligence, work, power imbalance and democracy – why co-determination is essential*, in *Italian Labour Law E-Journal*, 2021, 14(2), 157; DE STEFANO V., DOELLGAST V., *Introduction to the Transfer special issue. Regulating AI at work: labour relations, automation, and algorithmic Management*, in *Transfer*, 2023, 29(1), 9.
[16] Per esempio, può ipotizzarsi, laddove non ricorrano i requisiti dimensionali dell'impresa a cui la legge riconduce l'operatività dei diritti di informazione e consultazione.

di informazione con tale finalità, lasciando impregiudicati i diritti esistenti dei lavoratori". L'impressione è che il legislatore, così affermando, dimostri di non aver assimilato la distinzione funzionale tra le due categorie di diritti di informazione a cui alludevo poc'anzi, ed anzi le confonda.

Un ulteriore errore prospettico imputabile al Regolamento, in una logica lavoristica, è l'avere escluso i sistemi di IA utilizzati nell'ambito dei rapporti di lavoro dall'obbligo, che l'art. 27 pone in capo ai *deployer*, di effettuare una valutazione di impatto sulla possibile violazione dei diritti fondamentali. La valutazione d'impatto è, infatti, anche nella logica prettamente procedurale adottata dall'*AI Act*, uno strumento cruciale di controllo e corretta implementazione dell'IA, e, quindi di rafforzamento dei diritti[17].

Infine, un cenno alla sfera dei rimedi. La norma centrale a questo riguardo è l'art. 86, che attribuisce a qualsiasi persona destinataria ("oggetto") di una decisione adottata nell'ambito di un sistema ad alto rischio, e che si ritenga aver esercitato un impatto negativo sulla sua salute, sicurezza o sui suoi diritti fondamentali il diritto di ottenere dal *deployer* spiegazioni chiare e significative sul ruolo del sistema di IA nella procedura decisionale e sui principali elementi della decisione adottata. L'introduzione di un diritto alla spiegazione rappresenta un avanzamento rispetto alla bozza originaria del Regolamento. Permangono, tuttavia, almeno due profili di criticità: in primo luogo, il diritto si arresta alla richiesta di spiegazioni, e nulla si dice di quali strumenti di tutela disponga il destinatario della decisione laddove la spiegazione non lo soddisfi[18]; in secondo luogo, il titolare del diritto è solo la persona fisica direttamente colpita dalla decisione, e mancano spazi espliciti per un supporto sindacale o comunque collettivo.

In sintesi, il sistema di prevenzione e mitigazione dei rischi disegnato dal Regolamento presta il fianco a numerose critiche in chiave giuslavoristica: esso appare sbilanciato verso gli obblighi del fornitore, non prende in piena considerazione le specificità del rapporto di lavoro e rischia di veicolare surrettiziamente il messaggio della deresponsabilizzazione del datore/*deployer* una volta che costui abbia seguito correttamente le istruzioni che gli sono state fornite.

Più ombre che luci, quindi? Forse tale conclusione sarebbe affrettata. Non bisogna, infatti, trascurare due considerazioni. La prima è che l'*AI Act* non è una normativa lavoristica. Non

[17] Sul punto, ampiamente, PERUZZI M., *op. cit.*
[18] Per la critica alla mancanza, nell'*AI Act*, di un apparato sanzionatorio adeguato alla difesa dei diritti dei lavoratori cfr. ALAIMO A., *Il Regolamento sull'Intelligenza Artificiale: dalla proposta della Commissione al testo approvato dal Parlamento. Ha ancora senso il pensiero pessimistico?*, in *Federalismi.it*, Focus Lavoro, Persona, Tecnologia 18 ottobre 2023.

a caso, la sua base giuridica non risiede nel "capitolo sociale" del TFUE, bensì nelle norme sul mercato comune e la concorrenza. Non si può chiedere pertanto all'*AI Act* ciò che non può dare. La seconda è che l'*AI Act* non è isolato nell'ordinamento. Esso è parte di un'"architettura normativa integrata"[19] che comprende un apparato specificamente lavoristico, ancora in costruzione ma che già consta di alcuni capisaldi, con il quale il Regolamento dovrà essere messo a sistema.

Di tale apparato fanno parte, innanzitutto, il GDPR, che è oggetto di numerosi tra i contributi che seguono, e la normativa in materia di prevenzione dei rischi per la salute e la sicurezza nei luoghi di lavoro. Ci sono inoltre i diritti di informazione e consultazione di cui alla direttiva-quadro 2002/14, pienamente applicabili in caso di adozione di un sistema di IA, trattandosi di una circostanza che rientra nella nozione di "decisioni suscettibili di comportare cambiamenti di rilievo in materia di organizzazione del lavoro" posta dall'art. 4, comma 1, lett. c). Ci sono poi i diritti di trasparenza introdotti con il d.lgs. n. 104/22, che definiscono in modo molto più dettagliato del Regolamento i contenuti delle informazioni da rendere rispetto al funzionamento dei sistemi di decisione e monitoraggio automatizzati, e sui quali la giurisprudenza ha già iniziato a svolgere la sua funzione interpretativa. C'è la nuovissima direttiva sul lavoro tramite piattaforme digitali, che, pur avendo un campo di applicazione settoriale, delinea un sistema di tutele per il "management algoritmico" che ben potrebbe fungere da prototipo per il lavoro in generale. La direttiva stabilisce un quadro di divieti più esteso rispetto al Regolamento, e impone una serie di obblighi legati alla supervisione e alla revisione umana delle decisioni che, rispetto al Regolamento, offrono maggiori garanzie ai lavoratori (per esempio l'obbligo datoriale di modificare la decisione viziata e, soprattutto, il coinvolgimento dei rappresentanti dei lavoratori nel monitoraggio). C'è infine, ma non da ultimo, il diritto antidiscriminatorio, che offre un potenziale di maggiore effettività delle tutele attraverso, ad esempio, la semplificazione dell'onere probatorio per le vittime di un'asserita discriminazione e l'intervento processuale dei rappresentanti dei lavoratori.

Posto in questa luce, l'*AI Act* non sembra, invero, suscitare timori circa un potenziale effetto di arretramento delle tutele lavoristiche a fronte dell'avanzare di un orientamento legislativo eccessivamente *market-friendly* in materia di intelligenza artificiale. Occorrerà comunque lavorare allo sviluppo di una adeguata "sensibilità lavoristica" nell'interpretazione e nell'attuazione di questo strumento. Obiettivo che potrà essere perseguito con varie

[19] Così PERUZZI M., *op. cit.*, 36.

strategie: attraverso la "contaminazione" con le altre fonti; facendo sì che la figura datoriale non veda "diluirsi" il proprio ruolo a fronte degli altri attori del sistema di *governance*, e che quindi il concorso di ulteriori figure, quali i fornitori, determini un rafforzamento dell'apparato di tutela e non una semplice redistribuzione "a somma zero" delle responsabilità; e, infine, con un adeguato sostegno all'autonomia collettiva e alle relazioni industriali, fondamentali veicoli di gestione e di integrazione delle regole.

L'IA ACT NELLA PROSPETTIVA DEL DIRITTO COSTITUZIONALE: PRIME NOTAZIONI

Noemi Miniscalco
Assegnista di ricerca in Istituzioni di diritto pubblico nell'Università degli studi di Modena e Reggio Emilia

SOMMARIO: 1. Intelligenza artificiale e diritto costituzionale: una prospettiva di analisi muovendo dal *risk based approach*. - 2. I capisaldi (e limiti) di una IA affidabile e antropocentrica. - 3. La valutazione di impatto sui diritti fondamentali. - 4. Riflessioni conclusive.

1. Intelligenza artificiale e diritto costituzionale: una prospettiva di analisi muovendo dal *risk based approach.*

Di intelligenza artificiale[20] si parla oramai diffusamente da tempo, eppure solo di recente ha trovato definizione (e definitiva approvazione) il primo atto normativo vincolante (al mondo) diretto a regolare tale fenomeno[21]. Il che per la verità non stupisce se solo si considerano la velocità, l'ubiquità, finanche le incerte possibilità di sviluppo caratterizzanti tale famiglia di tecnologie, cui consegue la non facile individuazione e adozione da parte del legislatore di norme giuridiche, per loro natura destinate a perdurare nel tempo e produrre effetti in spazi definiti[22].

A fronte di tali elementi, il nuovo regolamento merita particolare attenzione, avendo superato, almeno per coloro che si trovano nel territorio dell'Unione[23], quell'irrisolto assetto dei rapporti tra diritto e tecnologia che in prospettiva radicale, come pure rilevato da taluni, avrebbe potuto finanche portare a "indebolire o addirittura ad annullare la funzione naturale

*Lo scritto rappresenta la versione rivista e aggiornata della relazione svolta il 14 maggio 2024, in occasione dell'incontro di studi "Lavoro, impresa e nuove tecnologie dopo l'AI Act".

[20] Di seguito, per brevità, anche semplicemente "IA".

[21] È noto che la Commissione europea ha presentato nel 2021 una proposta di Regolamento denominata "laying down harmonised rules on AI (Artificial Intelligence Act) amending certain Union legislative acts" (di seguito, nelle note e nel testo, per brevità, anche semplicemente "regolamento"), sulla quale però solo l'8 dicembre 2023 è stato raggiunto un accordo politico. A seguire, il 13 marzo 2024 il Parlamento europeo ha approvato in prima lettura un testo contenente emendamenti alla proposta della Commissione, cui è poi seguito il voto del Consiglio, il 21 maggio 2024. I richiami delle norme del regolamento contenuti in questo scritto fanno riferimento al testo recante gli emendamenti del Parlamento europeo. Nel momento in cui si scrive (maggio 2024) non è, infatti, ancora terminato il lavoro dei giuristi revisori.

[22] In tal senso, alla territorialità delle norme si oppone l'atopia della tecnica, come evidenzia IRTI N., *Norma e luoghi. Problemi di geo-diritto*, Laterza, Roma-Bari, 2006, 60 s. e 135 ss. In senso analogo, con riferimento ai nuovi poteri privati CASONATO C., *Potenzialità e sfide dell'intelligenza artificiale*, in *Biolaw Jurnal*, 2019, 178 afferma che "il potere economico legato alla disponibilità dei dati, come altri nella società globalizzata, non è facilmente localizzabile né inquadrabile all'interno di regole nazionali".

[23] Sebbene il regolamento presenti anche una vocazione extraterritoriale (cfr. art. 2).

e originaria del diritto"[24] stesso.

Ora, tra i diversi profili di rilievo che la nuova disciplina solleva nell'ottica del diritto costituzionale[25], provando a rispondere a quanto ci è stato richiesto e comunque considerato il tema del convegno, intendiamo guardare al regolamento nella prospettiva dei diritti e dell'impatto dell'IA su essi, individuando le norme ove il legislatore ha delineato quel contemperamento tra l'interesse alla diffusione di sistemi intelligenti, da un lato, e la protezione dei diritti e delle libertà dell'uomo, dall'altro lato; interessi che, di fatto, trovano sintesi nell'ambizione, chiaramente esplicitata nell'art. 1 del regolamento, alla promozione di un'intelligenza artificiale antropocentrica e affidabile[26].

A muoverci in tale scelta di indagine è la convinzione che l'analisi dell'impatto dell'attuale sviluppo tecnologico sui diritti dell'uomo e correlativamente l'individuazione di misure di tutela di essi sono una possibile risposta, se non anche la sola risposta possibile, di regolazione dei nuovi fenomeni emergenti, ancor più in considerazione della rilevante estensione degli ambiti di impiego di sistemi di intelligenza artificiale e dell'ormai acquisita consapevolezza che dall'innovazione possono derivare non solo dei benefici per le persone, ma pure diversi rischi a seconda dell'uso e dell'impiego che dei suoi prodotti e servizi venga fatto[27].

Del resto, già a livello costituzionale quella medesima tensione tra sviluppo tecnologico e persona è rintracciabile in diverse norme. Così, per esempio, nell'art. 9 della Carta che, sebbene inizialmente aveva portato persino a dubitare "della possibilità di ritrovarvi un qualche significato giuridico"[28] finanche ritenendo già tutelati gli interessi in esso sanciti in altre norme costituzionali, in tempi più recenti ha finito per assumere una forte centralità,

---

[24] Così, CHELI E., *Scienza, tecnica e diritto: dal modello costituzionale agli indirizzi della giurisprudenza costituzionale*, in *Rivista AIC*, n. 1, 2017, 9, che specifica che ciò è vero specie se si concorda nel ritenere "che questa funzione attiene alla cura della "antropologia profonda della specie umana", cioè alla difesa dell'integrità della persona". L'espressione "antropologia profonda della specie umana" è di RODOTÀ S., *Il diritto di avere diritti*, Laterza, Roma-Bari, 2012, 345.

[25] Il fenomeno dell'IA incide infatti fortemente e in modo trasversale su tutti i principali profili del diritto costituzionale. Così, per esempio, in relazione al sistema delle fonti, anzitutto per le peculiarità del regolamento che costituisce un'eccezione rispetto alla generale tendenza a prediligere strumenti di *soft law* (sul punto, spec. ACETO DI CAPRIGLIA A., *Intelligenza artificiale: una sfida globale tra rischi, prospettive e responsabilità. Le soluzioni assunte dai governi unionale, statunitense e sinico. Uno studio comparato*, in *Federalismi.it*, 17 aprile 2024, 4), ma pure rispetto al comunque necessario intervento statale che l'atto che ci è stato consegnato richiede, così come rispetto alla forma di Stato e di governo, intesa come distribuzione dei poteri all'interno dell'ordinamento costituzionale, considerato il ruolo dei poteri privati in relazione allo sviluppo tecnologico. Per una più ampia ricostruzione, v., per tutti, SIMONCINI A., *La dimensione costituzionale dell'Intelligenza Artificiale*, in CERRINA FERONI G., FONTANA C., RAFFIOTTA E. C. (a cura di), *AI Anthology. Profili giuridici, economici e sociali dell'intelligenza artificiale*, il Mulino, Bologna, 2022, 135 ss.

[26] Cfr. art. 1 del regolamento.

[27] Nello stesso senso, tra gli altri, SIMONCINI A., *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *Biolaw journal*, 2019, 63 ss. e CASONATO C., *Per una intelligenza artificiale costituzionalmente orientata*, in D'ALOIA A. (a cura di), *Intelligenza artificiale e diritto. Come regolare un mondo nuovo*, Franco Angeli, Milano, 2020, 131 ss.

[28] Testualmente, CARAVITA B., *Art. 9*, in CRISAFULLI V., PALADIN L. (a cura di), *Commentario breve alla Costituzione*, Cedam, Padova, 1990, 51.

anche alla luce delle attuali caratteristiche della tecnologia[29]. E ciò tanto per la presenza nell'articolo *de quo* del lemma "ecosistema", che letto estensivamente sarebbe riferibile anche al mondo digitale[30], quanto – come riteniamo preferibile – se di esso si proceda con un'interpretazione in combinato disposto con altre norme[31] e segnatamente, tra esse, l'art. 41 Cost. Proprio in quest'ultima disposizione, infatti, è rintracciabile quell'equilibrio per cui lo sviluppo tecnologico, pure espressione di libertà di iniziativa economica, non è privo di limiti: esso piuttosto non può svolgersi in contrasto con l'utilità sociale o in modo da recare danno alla salute, all'ambiente, alla sicurezza, alla libertà e dignità dell'uomo. Secondo tale lettura, insomma, la riaffermazione di quegli obblighi esterni di finalizzazione induce ad una visione assiologica per cui l'innovazione e l'avanzamento nel settore della tecnologia sono interessi che vanno sì tutelati, ma pure ragionevolmente contemperati con altri beni di pari rango, nell'ottica primaria del pieno sviluppo della persona umana[32].

Un approccio non dissimile è rintracciabile nel regolamento di cui andiamo, ora, ad occuparci: in tale atto, coerentemente con le scelte già operate in altre fonti con cui il legislatore ha inteso normare la società digitale[33], traspare la consapevolezza non più solo dei benefici ma pure dei rischi per l'uomo che possono derivare dallo sviluppo ed uso dei prodotti e servizi della tecnica e, specificamente, dai sistemi di intelligenza artificiale[34]; rischi da cui il legislatore muove per individuare regole che rispondano in modo graduale ai diversi contesti ed usi possibili dei sistemi di IA, tenuto conto della probabilità di verificazione di

[29] In argomento, per una più ampia ricostruzione, sia consentito rinviare a MINISCALCO N., *L'intelligenza artificiale in movimento. L'impatto della* smart mobility *sui diritti costituzionali*, Walters Kluwer, Milano, 2024, 60 ss.

[30] In senso a questo affine, la prospettiva di SIMONCINI A., *Il linguaggio dell'Intelligenza Artificiale e la tutela costituzionale dei diritti*, in *Rivista AIC*, 2023, n. 2, 4, che declina la nozione di "ecosistema" "affiancando agli organismi viventi di natura organica (persone, animali e vegetali) organismi cognitivo-relazionali di natura inorganica (macchine sociali), fino a comprendere anche l'integrazione biomeccanica dei due (la cosiddetta prospettiva "cyborg")".

[31] Con specifico riferimento ai sistemi di intelligenza artificiale, CASONATO C., *Costituzione e intelligenza artificiale: un'agenda per il prossimo futuro*, in *Consulta Online*, 13 gennaio 2020, evidenzia come i principi delineati negli artt. 9, 33 e 41 Cost. "possono costituire un'efficace cornice entro cui inserire una regolamentazione dell'AI costituzionalmente orientata, che la indirizzi verso scopi di progresso scientifico, economico e sociale, oltre che di generale benessere" (spec. 12). Più in generale, sulla convivenza tra libertà economiche e altri interessi v., *ex multis*, NANIA R., *Libertà economiche: impresa e proprietà*, in ID., RIDOLA P. (a cura di), *I diritti costituzionali*, vol. I, Giappichelli, Torino, 2006, 194 ss.

[32] Pone l'accento sul carattere non assoluto dello sviluppo della tecnica, in ragione della sussistenza di un coacervo di contro-interessi, LA ROSA E., *Libertà di ricerca scientifica come limite all'intervento penale?*, in PANELLA L. (a cura di), *Nuove tecnologie e diritti umani: profili di diritto internazionale e di diritto interno*, Editoriale Scientifica, Napoli, 2018, 313.

[33] Per un'ampia e precisa ricostruzione di tali fonti, v. IANNUZZI A., *Le fonti del diritto dell'Unione europea per la disciplina della società digitale*, in PIZZETTI F. (a cura di), *La regolazione europea della società digitale*, Giappichelli, Torino, 2024, spec. 10 s.

[34] Ai sensi dell'art. 3, par. 1, n.1, un "sistema di IA" è "un sistema automatizzato progettato per funzionare con livelli di autonomia variabile e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali".

danni per i diritti dell'uomo e della gravità di essi[35].

In tal senso, infatti, a fronte di rischi inaccettabili, il legislatore ha vietato alcuni possibili impieghi dei sistemi di intelligenza artificiale in diversi settori[36], prevedendo invece adempimenti specifici per i sistemi ad alto rischio[37], cui è dedicata la più parte della disciplina, così come per i modelli di IA per finalità generali che presentino un rischio sistemico, ed introducendo, infine, regole armonizzate in materia di trasparenza, nonché la possibile adozione di codici di condotta in presenza di rischi meno elevati.

L'approccio basato sul rischio, insomma, tiene conto dei risultati positivi sul piano sociale e ambientale che i sistemi di IA possono apportare, ma pure delle (possibili) conseguenze negative che queste tecnologie possono generare: esso è il meccanismo flessibile utilizzato per bilanciare, in modo proporzionale, libertà e limiti dello sviluppo tecnologico per finalità sociali, laddove il rischio diventa il parametro di misura sulla base del quale il contemperamento si sposta nell'una o nell'altra direzione.

Ebbene, proprio in linea con tale approccio, il legislatore ha individuato in alcune disposizioni, più di altre, i tratti essenziali e imprescindibili che dovranno caratterizzare i sistemi di IA, affinché possano dirsi (o almeno tendano ad essere) effettivamente affidabili e antropocentrici. Si tratta di disposizioni che – pur non essendo qualificate come tali – assurgono a ruolo di principi, rappresentando il perno dell'intero sistema delineato; di esse, andiamo allora ad occuparci.

2. I capisaldi (e limiti) di una IA affidabile e antropocentrica.

Affinché i sistemi di IA ad alto rischio possano dirsi affidabili e antropocentrici, essi dovranno essere progettati (e successivamente impiegati) in modo da essere conformi alle disposizioni in materia di: *governance* dei dati (art. 10), trasparenza (art. 13), sorveglianza umana (art. 14), accuratezza, robustezza e cybersicurezza (art. 15).

In relazione al primo di tali principi, non possiamo che muovere da una premessa: alla base del funzionamento di queste tecnologie vi sono i dati ed è noto che l'impiego di tale

[35] Il rischio andrebbe analizzato ponendo mente "alla salute, alla sicurezza o ai diritti fondamentali delle persone fisiche"; così la lettera di cui agli artt. 6 par. 3 e par. 6, e 7 par. 1 lett. b) del regolamento.

[36] I sistemi a rischio inaccettabile, individuati all'art. 5 del regolamento, salvo deroghe espresse, sono per esempio quelli che: utilizzano tecniche subliminali; sfruttano le vulnerabilità di un gruppo specifico di persone, dovute all'età o alla disabilità; che inferiscono le emozioni di una persona fisica nell'ambito del luogo di lavoro e degli istituti di istruzione; nonché i sistemi di c.d. *social scoring* impiegati da Autorità pubbliche.

[37] Cfr. art. 6 e allegato III del regolamento. Rientrano, per esempio, in questa categoria i sistemi usati per la valutazione degli studenti, i sistemi di IA destinati a essere utilizzati per l'assunzione o la selezione di persone fisiche, oppure per adottare decisioni riguardanti le condizioni dei rapporti di lavoro, la promozione o cessazione dei rapporti contrattuali di lavoro; i sistemi predittivi in ambito penale o, ancora, quelli di gestione dell'immigrazione.

asset porta ad emersione il rischio di possibili distorsioni, tanto rispetto al funzionamento stesso dei sistemi, quanto al risultato cui essi pervengono e dunque in relazione all'*output* dei processi. In ragione di ciò, l'art. 10 del regolamento sancisce, per l'ipotesi in cui i sistemi utilizzino tecniche di apprendimento che impieghino dati, che l'individuazione dei *set* per l'addestramento (*data set*) per la convalida (*convalidation set*) e per la prova (*test set*) devono essere selezionati in modo da essere pertinenti, rappresentativi, anche tenuto conto delle specifiche dell'area geografica di applicazione, e, nella misura del possibile, esenti da errori e completi[38].

Tra le ulteriori misure indicate nell'ottica della *governance* dei dati, vi sono il monitoraggio, il rilevamento e la correzione delle distorsioni o *bias*, considerato che l'uso dei sistemi di IA può aumentare il rischio di discriminazione, a seconda di come "vengano definite le variabili target del modello, di come vengano selezionate le caratteristiche del modello di apprendimento, e degli elementi sostitutivi (proxy)"[39].

Diversi sono i casi in cui, come noto, l'impiego dei sistemi di IA ha determinato effetti distorsivi; tra essi, basti pensare all'algoritmo utilizzato da Uber attraverso il quale la retribuzione dei lavoratori veniva calcolata utilizzando criteri quali il tasso di disponibilità e la valutazione dei clienti i quali potevano essere soggetti a distorsioni a causa di stereotipi (per esempio di non affidabilità delle donne al volante) che crea(va)no disuguaglianza, oppure all'algoritmo di Amazon che classificava i dipendenti tramite *set* di dati di addestramento basati sui profili di dipendenti assunti in precedenza e che discriminava in fase di selezione[40].

La non discriminazione algoritmica che, come abbiamo evidenziato, deve essere assicurata anzitutto attraverso l'adeguata selezione e il corretto uso dei dati nel rispetto di quanto previsto dall'art. 10 del regolamento, trova peraltro riferimenti pure in altri addentellati normativi e, tra essi, nell'art. 5 che vieta alcune pratiche di IA proprio per l'effetto distorsivo che esse rischiano di generare[41], o nell'art. 77 in relazione ai poteri delle autorità o degli organismi pubblici nazionali che tutelano i diritti fondamentali, ove tra questi ultimi viene

[38] Peraltro, alcune pratiche di *governance* dei dati devono essere implementate pure per i sistemi di IA ad alto rischio che non si basano sull'addestramento automatico.

[39] CONTISSA G., GALLI F., GODANO F., SARTOR G., *Il regolamento europeo sull'intelligenza artificiale. Analisi informatico-giuridica*, in *i-lex*, 2021, n. 2, 23.

[40] Con maggior precisione, in tal caso si era innanzi ad una *proxy discrimination*, poiché pur non essendo né il genere né l'etnia parte dell'insieme di variabili inserite nel modello, l'algoritmo autonomamente correlava queste caratteristiche ai candidati. Su tali profili e per un maggiore approfondimento si vedano, in diverse prospettive, almeno, NARDOCCI C., *Intelligenza Artificiale e discriminazioni*, in COSTANZO P., MAGARÒ P., TRUCCO L. (a cura di), *Il diritto costituzionale e le sfide dell'innovazione tecnologica. Atti del Convegno di Genova del 18-19 giugno 2021*, Editoriale Scientifica, Napoli, 2022, 241-299 e GAUDIO G., *Le discriminazioni algoritmiche*, in *LDE*, 2024, n.1, 1 ss.

[41] Basti pensare al divieto di immissione sul mercato, messa in servizio o uso di sistemi di IA che sfruttino "le vulnerabilità di una persona o di uno specifico gruppo di persone, dovute all'età, alla disabilità o a una specifica situazione sociale o economica, con l'obbiettivo o l'effetto di distorcer(n)e materialmente il comportamento" (art. 5, par. 1, lett. b) del regolamento).

compreso espressamente il diritto alla non discriminazione algoritmica.

Parallelamente ai processi di gestione dei dati, i sistemi di IA ad alto rischio soggiacciono a regole di trasparenza, le quali sono peraltro previste, seppure in via differenziata, per tutti i soggetti coinvolti nella catena del valore dell'IA. A venire in rilievo è, in primo luogo, il disposto di cui all'art. 13 del regolamento, secondo cui i sistemi *de quibus* devono essere progettati e sviluppati in maniera tale che il loro funzionamento sia sufficientemente trasparente per i *deployer*, di modo che questi possano interpretarne l'*output* e utilizzarlo adeguatamente. A tal fine, i sistemi di IA ad alto rischio devono essere accompagnati da istruzioni per l'uso, che comprendano informazioni concise, complete, corrette, chiare, pertinenti, accessibili e comprensibili[42].

La trasparenza opera, peraltro, trasversalmente: l'art. 50 del regolamento, nel prevedere taluni obblighi per i fornitori e i *deployer* di determinati sistemi di IA, sancisce che, quando un sistema sia destinato ad interagire con persone fisiche, queste ultime devono essere informate del fatto che stanno utilizzando tale sistema. Del pari, i fornitori di sistemi di IA, compresi i sistemi di IA per finalità generali, che generano contenuti audio, immagine, video o testuali sintetici, devono garantire che gli *output* del sistema stesso siano marcati in un formato leggibile meccanicamente e rilevabili come generati o manipolati artificialmente.

L'interpretabilità dell'*output* da parte del *deployer*, di cui all'art. 13 su richiamato, non va confusa con la spiegabilità del risultato[43], che va riferito più ampiamente alla possibilità di comprensione dei processi di elaborazione effettuati dai sistemi.

A tal riguardo, non si rinviene nel regolamento un obbligo generale di trasparenza/spiegabilità, quanto piuttosto un obbligo specifico di spiegazione dei processi decisionali in relazione alle persone fisiche soggette ad una decisione automatizzata. Ai sensi dell'art. 86 del regolamento, infatti, qualsiasi persona oggetto di una decisione adottata da un *deployer* sulla base dell'*output* di un sistema di IA ad alto rischio, fatte salve talune eccezioni, ha il diritto di ottenere spiegazioni chiare e significative sul ruolo del sistema di IA nella procedura decisionale e sui principali elementi della decisione adottata.

L'art. 86, peraltro, va letto alla luce dell'art. 22 del Regolamento UE 2016/679 (di seguito, anche, semplicemente "GDPR")[44], che prevede, salvo eccezioni, il diritto dell'interessato "di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato,

[42] L'elenco delle informazioni minime che devono essere contenute nelle istruzioni per l'uso è previsto nell'art. 13, par. 3, del regolamento.
[43] Su tali aspetti v., almeno, SARTOR G., *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*, Study PE 641.530, European Parliamentary Research Service, 2020.
[44] In argomento, v., *ex multis*, LAGIOIA F., SARTOR G., SIMONCINI A., *Art. 22*, in D'ORAZIO R., FINOCCHIARO G., POLLICINO O., RESTA G. (a cura di), *Codice della privacy e data protection*, Giuffrè, Milano, 2021, 378 ss.

compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona". Poiché nelle ipotesi in cui la decisione automatizzata può dirsi lecita ai sensi del GDPR, il diritto di ottenere l'intervento umano (che è ovviamente cosa diversa dal diritto di ottenere una spiegazione sul ruolo del sistema di IA), nonché di esprimere la propria opinione e di contestare la decisione è assicurato per le sole ipotesi di cui al paragrafo 2, lettere a) e c) dell'art. 22 poc'anzi citato e non invece allorquando la decisione sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, in relazione ai trattamenti automatizzati effettuati dai sistemi di IA ammessi dal nuovo regolamento sembrerebbe assistersi ad un detrimento di tutela per la persona interessata dalla decisione stessa.

Sennonché, in relazione all'intervento umano, particolare attenzione merita l'art. 14 del regolamento che, nel prevedere specifiche misure di sorveglianza umana, sancisce che i sistemi di IA ad alto rischio devono essere progettati e sviluppati, anche con strumenti di interfaccia uomo-macchina adeguati, che ne permettano la supervisione da parte di persone fisiche, al fine di prevenire o ridurre al minimo i rischi per i diritti. Limitandoci solo ad alcuni profili, rilevante è la previsione per cui le misure di sorveglianza devono assicurare alle persone cui è affidata la supervisione dei sistemi suddetti di: a) comprendere correttamente le capacità e i limiti pertinenti di essi così da poterne monitorare il funzionamento anche per poter intervenire in caso di anomalie o malfunzionamenti; b) rimanere consapevole dell'uso di un sistema di IA, in modo tale da non incorrere nella c.d. distorsione automatica ossia nel rischio di fare eccessivo affidamento sul risultato del sistema stesso, ancor più se l'output consiste in informazioni o raccomandazioni per le decisioni che devono essere prese da persone fisiche[45]; d) interpretare correttamente l'*output*; e) decidere di non usare il sistema o di ignorare, annullare o di discostarsi dal risultato del sistema; e) intervenire sul funzionamento e interromperne il funzionamento mediante specifico pulsante di arresto.

A destare interesse è anche il par. 5 dell'articolo 14 del regolamento che reca espressamente il principio di non esclusività della decisione algoritmica "per i sistemi di IA ad alto rischio di cui all'allegato III, punto 1, lett. a)", ossia i sistemi di identificazione biometrica remota, prevedendo in aggiunta alle altre misure di sorveglianza umana anche che "il *deployer* non compia azioni o adotti decisioni sulla base dell'identificazione risultante dal sistema, a meno che tale identificazione non sia stata verificata e confermata separatamente da almeno due persone fisiche dotate della necessaria competenza, formazione e autorità".

[45] In argomento, LAGIOIA F., CONTISSA G., *The Strange Case of Dr. Watson: Liability Implications of AI Evidence-Based Decision Support Systems in Health Care*, Eur. J. Legal Stud., 2020, n. 12, 281.

Nella sostanza, nell'individuazione delle misure di sorveglianza umana il concetto di decisione è sempre riferito ad almeno una persona fisica, in ragione del fatto che l'*output* del sistema può al più consistere in informazioni o raccomandazioni per le decisioni stesse, salvo l'ipotesi di cui al par. 5 per la quale si prevede l'intervento di almeno due persone.

Ora, per la verità, tale assetto normativo che, in astratto, afferma e conferma il ruolo primario della persona umana nell'uso dei sistemi di IA rischia di essere però, in concreto, inefficace, in ragione di quel presupposto di comprensione e spiegazione del funzionamento dei sistemi (la c.d. *explainable/explicable* AI) che, come noto, risulta particolarmente problematico. La questione è, in altri termini, quella delle *black box*, caratterizzate da intrinseca opacità, che renderebbe incomprensibile (se non finanche impossibile) per l'essere umano di ricostruire il processo seguito dalla macchina per giungere ad un determinato risultato[46]. Il che assume specifico rilievo anzitutto rispetto alla ricerca di *standard* e modalità tecniche che consentano di includere nella progettazione degli algoritmi meccanismi di tracciamento e controllo[47], ma pure rispetto al livello adeguato di profondità di conoscenza del processo stesso, sempre che si riesca, a monte, a conoscerne e comprenderne il funzionamento[48].

Da ultimo, pur non potendo che limitarci ad un mero cenno, un ruolo importante è quello assunto dall'art. 15 del regolamento che prevede che i sistemi devono essere progettati e sviluppati in modo da assicurare un adeguato livello di accuratezza, robustezza e cybersicurezza durante tutto il loro ciclo di vita. A tal fine, un ruolo fondamentale assumono le misure di sicurezza tecniche e organizzative che devono essere adottate al fine di rendere i sistemi suddetti il più resilienti possibile per quanto riguarda errori, malfunzionamenti o incongruenze. Laddove peraltro un'attenzione specifica va posta agli *output*, in relazione ai quali occorre ridurre il più possibile il rischio di distorsioni, ancor più quando il risultato stesso costituisce *input* per operazioni future.

3. La valutazione di impatto sui diritti fondamentali.

Seguendo la linea sin qui tracciata, nella nuova disciplina vi è una norma specifica che esprime chiaramente quell'esigenza di porre al centro del sistema l'uomo e i suoi diritti, a fronte dei rischi che possono emergere dall'impiego dei sistemi di IA: è l'art. 27 del regolamento e la previsione in esso dell'obbligo di valutazione di impatto sui diritti

[46] In argomento, PASQUALE F., *The black box society: The secret algorithms that control money and information*, Harvard University Press, Cambridge-London, 2015.
[47] Cfr. VILONE G., LONGO L., *Notions of Explainability and Evaluation Approaches for Explainable Artificial Intelligence*, in *Information Fusion*, 2021, n. 76, 89 ss.
[48] Su tale profilo, per esempio, è stata prospettata l'opportunità di conoscere le inferenze e le opinioni che gli algoritmi creano sulla base di dati personali; cfr. WACHTER S., MITTELSTADT B., *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, in *Columbia Business Law Review*, 2019, n. 2, 1 ss.

fondamentali per i sistemi di IA ad alto (anche nota come *Fundamental Rights Impact Assessment* o "FRIA").

La norma sancisce in particolare che, prima dell'utilizzo di un sistema di IA ad alto rischio, i *deployer* che sono organismi di diritto pubblico o enti privati che forniscono servizi pubblici, così come i *deployer* di sistemi di IA destinati a essere utilizzati per valutare l'affidabilità creditizia delle persone fisiche o per stabilire il loro merito di credito, a eccezione dei sistemi di IA messi in servizio per uso proprio da fornitori di piccole dimensioni oppure destinati a essere utilizzati per inviare servizi di emergenza di primo soccorso o per stabilire priorità in merito all'invio di tali servizi, devono effettuare una valutazione sull'impatto che l'uso del sistema può produrre sui diritti fondamentali. Eventualmente, in casi analoghi, essi potranno basarsi su valutazioni d'impatto precedentemente condotte o su quelle, se esistenti, effettuate dal fornitore, sebbene tale adempimento richieda comunque un monitoraggio continuo e sistematico.

Ora, limitandoci a talune considerazioni, anzitutto tale adempimento, che non era presente nella proposta di regolamento presentata dalla Commissione europea e che è stato introdotto con appositi emendamenti dal Parlamento UE, ha finito per essere ricalibrato nell'accordo finale. In quest'ultimo, invero, è stato limitato l'ambito di applicazione soggettivo dell'obbligo di valutazione, di modo che tale misura di garanzia risulta attualmente meno incisiva di quanto (era e) sarebbe stato, a nostro avviso, auspicabile, ancor più considerato che, di fatto, essa non vedrà i suoi effetti prodursi rispetto a quei fornitori che offrono servizi tecnologici privati, segnando un *favor* proprio per quei "nuovi" poteri che nel settore digitale incidono fortemente non solo sul mercato ma pure sui diritti. Peraltro, la stessa delimitazione soggettiva operata non è scevra di criticità: basti pensare al riferimento agli "organismi di diritto pubblico", in relazione al quale, non rinvenendosi una specifica definizione nell'atto normativo, viene da chiedersi se vada letto alla luce della disciplina europea dei contratti pubblici[49].

Meritorio di più attenta analisi è inoltre il rapporto tra l'adempimento di cui ci stiamo occupando e la valutazione di impatto sulla protezione dei dati personali (di seguito, anche, "DPIA") di cui all'art. 35 del Regolamento UE 2016/679. Ora, proprio in ragione della sovrapposizione possibile tra tali valutazioni, il regolamento prevede che esse si integrino

[49] Si consideri, peraltro, che anche il Regolamento UE 2016/679 solleva alcune criticità in punto di delimitazione soggettiva. È il caso, per esempio, della previsione di cui all'art. 37 che nella parte in cui, tra le altre ipotesi, pone in capo agli "organismi pubblici" l'obbligo di designazione del *Data Protection Officer*, utilizza un'espressione che rimane di incerta interpretazione nella misura in cui non è chiaro quando un ente, quand'anche rivesta forma privatistica, presenti caratteri pubblicistici tali da dover essere ricondotto in tale categoria. Per un'analisi sul punto – e una possibile lettura – sia consentito rinviare a MINISCALCO N., *Autorità pubblica e organismo pubblico nel Regolamento UE 2016/679 tra dubbi e incauti rimandi*, in *Dir. Inform.*, 2020, n. 2, 313-326.

reciprocamente[50] e pertanto potrebbe essere buona norma che esse vengano condotte, se del caso in documenti separati, ma congiuntamente.

A ben vedere, molteplici sono però le differenze tra i due adempimenti: l'ambito soggettivo di applicazione risulta essere maggiormente esteso per la DPIA; l'obbligo di notifica, salvo specifiche esenzioni, all'Autorità di vigilanza è previsto per la sola FRIA; del tutto parziale può dirsi, infine, la sovrapposizione tra i loro contenuti.

In relazione a tale ultimo aspetto, infatti, la DPIA ha un ambito materiale più ristretto della FRIA che presuppone che l'analisi venga compiuta su un maggiore assetto di interessi, sebbene – *en passant* – non sia del tutto chiaro se questi ultimi corrispondano a tutti i diritti individuati nella Carta dei diritti fondamentali dell'Unione europea, richiamata espressamente dall'art. 1 del regolamento, oppure, più limitatamente, se vada indagato l'impatto solo in relazione a quelli, tra essi, che effettivamente possono venire incisi dall'uso dei sistemi di IA, come parrebbe doversi supporre guardando alle metodologie ad oggi elaborate, tra le quali il Canada's Algorithmic Impact Assessment tool (AIA)[51] o il Fundamental Rights and Algorithms Impact Assessment (FRIA) proposto dal Ministro dell'Interno olandese[52] o, ancora, il Fundamental Right Assessment (AFRIA) realizzato nell'ambito del progetto Aligner[53].

Dubbi – questi – che saranno presumibilmente superati allorquando l'ufficio per l'IA elaborerà, come sancito dal par. 5 dell'art. 27, il modello di questionario per agevolare i *deployer* nell'adempimento di questo obbligo.

---

[50] Infatti, come sancito dall'art. 27, par. 4, "se uno qualsiasi degli obblighi di cui al presente articolo è già rispettato a seguito della valutazione d'impatto sulla protezione dei dati effettuata a norma dell'articolo 35 del regolamento (UE) 2016/679 o dell'articolo 27 della direttiva (UE) 2016/680, la valutazione d'impatto sui diritti fondamentali di cui al paragrafo 1 integra tale valutazione d'impatto sulla protezione dei dati".

[51] Esso è, in particolare, uno strumento a supporto delle autorità e organismi pubblici che fornisce una metodologia specifica per l'analisi dell'impatto derivante da un processo decisionale automatizzato. Per un approfondimento, v. GOVERNMENT OF CANADA, *Algorithmic Impact Assessment tool*, reperibile al link *https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html*, consultato il 21 maggio 2024.

[52] Il *Fundamental Rights and Algorithms Impact Assessment* (FRAIA) è una valutazione diretta all'analisi dei rischi per i diritti umani che derivano dall'uso di algoritmi, al fine dell'individuazione di misure per la limitazione dei rischi stessi. Cfr. GOVERNMENT OF THE NETHERLANDS, MINISTRY OF THE INTERIOR AND KINGDOM RELATIONS, *Impact Assessment Fundamental rights and algorithms*, marzo 2022, reperibile al link *https://www.government.nl/binaries/government/documenten/reports/2021/07/31/impact-assessment-fundamental-rights-and-algorithms/fundamental-rights-and-algorithms-impact-assessment-fraia.pdf*, consultato il 21 maggio 2024.

[53] Il *Fundamental Rights Impact Assessment* realizzato nell'ambito del progetto Aligner, finanziato con fondi Horizon 2020 dell'Unione europea (grant agreement n. 101020574) è un *tool* che permette di indagare l'impatto dei sistemi di IA e consiste in due modelli connessi e complementari: il *Fundamental Rights Impact Assessment template* e il *AI System Governance template*. Tali documenti sono reperibili sul sito internet della società al link *https://aligner-h2020.eu/fundamental-rights-impact-assessment-fria/*, consultato in data 21 maggio 2024.

4. Riflessioni conclusive.

Se è vero che lo sviluppo della tecnica porta tanto dei benefici quanto dei rischi, il legislatore europeo con il regolamento di cui ci siamo occupati nelle pagine precedenti manifesta sicuramente sensibilità e consapevolezza della necessità di veicolarne l'incedere in una direzione che sia, in ultima istanza, favorevole per l'uomo.

L'atto che ci è stato consegnato, risultato di un lungo periodo di gestazione, nel corso del quale diverse sono state le incertezze, a partire dalla stessa ampiamente dibattuta definizione di intelligenza artificiale[54], e da ultimo frettolosamente approvato, ci induce ad alcune riflessioni, di più ampio respiro, sulla capacità del regolamento di porsi quale presidio effettivo di garanzia per i diritti che esso pur mira a proteggere.

Limitandoci solo a talune considerazioni, rimane in primo luogo il problema di fondo della regolazione di fenomeni che cambiano rapidamente: "una regolazione adeguata alla realtà tecnologica è possibile solo a condizione che il regolatore segua costantemente l'evoluzione tecnologica"[55]. È vero che molteplici sono i rinvii a successivi interventi della Commissione europea, che con atti delegati e di esecuzione dovrà non solo specificare quanto nel regolamento previsto ma pure aggiornarne talune sue parti[56]. È però altresì vero che l'approccio seguito segna e cristallizza un modello di relazione tra diritto e tecnologia che vede il diritto intervenire (e non prevenire) la regolazione e gestione dei nuovi rischi emergenti[57]. A ciò si aggiunga che il regolamento diventerà pienamente applicabile, con alcune eccezioni, solo dopo 24 mesi dalla sua entrata in vigore, il che rende ben possibile che, ancor prima che il testo dispieghi piena efficacia, alcune sue previsioni risulteranno da integrare o modificare, al mutare della realtà stessa che esso intende regolare. Rispetto a tale aspetto, meritoria ci pare la promozione da parte della Commissione del c.d. patto sull'IA, attraverso il quale l'Istituzione sta cercando di convogliare – già dal mese di novembre 2023 con la pubblicazione del primo invito a manifestare interesse, che ha ottenuto più di cinquecentocinquanta risposte di diverse organizzazioni – l'impegno volontario dei diversi

[54] In particolare, sulla difficoltà di definizione dell'IA, SCHERER M. U., *Regulating Artificial Intelligence Systems: risks, challanges competencies, and strategies*, in *Harv. J.L. & Tech.*, 2016, n. 29(2), 359 ss.; TRINCADO CASTÁN C., *The legal concept of artificial intelligence: the debate surronding the definition of AI System in the AI Act*, in *BioLaw Journal – Rivista di BioDiritto*, 2024, n. 1, 305 ss. e riferimenti ivi citati.

[55] Richiamando le parole di PIZZETTI F., *Introduzione alla regolazione europea della società digitale*, in ID. (a cura di), *La regolazione europea della società digitale*, Giappichelli, Torino, 2024, 3.

[56] Cfr., a riguardo, per esempio, il considerando n. 52 (ma sul punto v. anche il considerando n. 53, 81, 173, 174, nonché gli artt. 6 par. 6 e 7) che, in relazione all'identificazione dei sistemi ad alto rischio, prevede che "la Commissione dovrebbe avere il potere di adottare, mediante atti delegati, per tenere conto del rapido ritmo dello sviluppo tecnologico nonché dei potenziali cambiamenti nell'uso dei sistemi di IA". In senso analogo, rispetto ai modelli di IA per finalità generali si vedano i considerando nn. 101, 111 nonché l'art. 52 par. 4.

[57] Il che potrebbe peraltro comportare un rischio di ipertrofia legislativa, in relazione al quale, sebbene in relazione alla regolazione dei dati, si veda TORREGIANI S., *La circolazione dei dati secondo l'ordinamento giuridico europeo. Il rischio dell'ipertrofia normativa*, in *RIID*, 2021, 49 ss.

portatori di interesse e degli operatori del settore per anticipare e avviare l'attuazione della nuova disciplina ancor prima dei termini previsti[58].

In secondo luogo, non possiamo sottovalutare come il regolamento rimane un atto dell'Unione europea che, pur con la sua vocazione extraterritoriale, troverà applicazione entro limiti spaziali o a garanzia delle persone che si trovino nel territorio dell'Unione.

Sul punto, peraltro, ci si conceda questo accenno, neppure l'adozione, il 17 maggio 2024, della Convenzione quadro sull'intelligenza artificiale e i diritti dell'uomo, la democrazia e lo stato di diritto, ad opera dei 46 Paesi membri del Consiglio d'Europa risponde davvero all'esigenza di una più complessiva regolazione del fenomeno di cui ci occupiamo. Pur essendo questo il primo atto di diritto internazionale, volto a garantire lo sviluppo dell'IA nel rispetto dei diritti fondamentali, non solo com'è ovvio esso dovrà essere trasposto dai legislatori a livello nazionale, ma pure risulta non dirimente sol che si pensi che oltre ai Paesi membri dell'UE, vi è sì la partecipazione anche di altri Stati, tra i quali gli Stati Uniti d'America, il Giappone e il Canada, ma non ovviamente della Cina.

Ora, tornando al recente intervento normativo eurounitario, se è vero – e a nostro avviso positivo – che l'Unione europea sta provando, anche con tale atto, a tutelare la propria sovranità digitale attraverso il ricorso a strumenti e poteri di regolazione, è pur vero che l'Europa è una terra di mezzo tra due potenze in punto di sviluppo tecnologico: gli USA[59] e la Cina[60]. Di più ed ampliando ulteriormente la prospettiva: essa è una terra che rimane nel mezzo, ma rischia di essere sempre più esclusa da quel "conflitto triadico" che intercorre tra USA, Cina e società tecnologiche mondiali[61].

L'Europa è insomma un attore nel settore dell'IA, non il solo, né il più rilevante; essa ha fatto però un primo passo, imperfetto, ma certamente importante[62]. Non possiamo che sperare che questo ispiri un cambio di rotta[63], all'insegna di una maggiore collaborazione su

---

[58] Le informazioni relative al Patto sull'IA sono reperibili sul sito istituzionale della Commissione europea, al link *https://digital-strategy.ec.europa.eu/it/policies/ai-pact*, consultato in data 21 maggio 2024.

[59] Il modello statunitense è noto essere quello di una regolazione più attenuata tendente alla auto-regolazione e basato sull'antitrust, frutto della preoccupazione "che un approccio normativo eccessivamente precauzionale possa inibire lo sviluppo dell'IA, facendo perdere terreno agli Stati Uniti, con implicazioni economiche, di sicurezza nazionale e complessivamente geopolitiche"; così, CASONATO C., MARCHETTI B., *Prime osservazioni sulla proposta di regolamento dell'Unione europea in materia di intelligenza artificiale*, in *BioLaw Journal*, 2021, 417.

[60] Diverso è invece il modello della Cina, espressione di dirigismo e del capitalismo di Stato; cfr., FINOCCHIARO G., *La regolazione dell'Intelligenza Artificiale*, in *Riv. Trim. Dir. Pubb.*, 2022, n. 4, 1091.

[61] In tal senso, IANNUZZI A., *Le fonti del diritto*, cit., 16, ma si vedano anche RODRIK D., *La globalizzazione intelligente*, Laterza, Roma-Bari, 2011, 263 ss. e CORNELLI V., *Sovranità tecnologica: intelligenza artificiale e valori costituzionali*, in *Forum di Quad. Cost.*, 2023, n. 2, spec. 60 ss.

[62] IANNUZZI A., *Le fonti del diritto*, cit., 14, ritiene che "la strada imboccata dall'Europa con questa decisa operazione di recupero della centralità delle fonti del diritto è quella giusta perché può consentire di affrontare correttamente il tema della sovranità e del potere nell'era digitale che rappresenta uno dei problemi più rilevanti del costituzionalismo del XXI secolo"

[63] Come è stato rilevato "nel contesto geopolitico […] la strategia dell'Unione europea è quella di porsi

tale tema, da parte di tutti i Paesi e i portatori di interessi, poiché le scelte che verranno prese pure da altri saranno fondamentali anche rispetto al nostro futuro.

come *leader* nella produzione normativa e far sì che il modello europeo divenga un riferimento globale e possa essere adottato nelle altre regioni del mondo (il cosiddetto "effetto Bruxelles")"; testualmente FINOCCHIARO G., *La regolazione dell'Intelligenza Artificiale*, cit., 1089 s. Sul c.d. effetto Bruxelles v., invece, BRADFORD A., *The Brussels Effect: How the European Union Rules the World*, Oxford University Press, New York, 2020.

IL REGOLAMENTO IA NEL SISTEMA DEL DIRITTO DEL LAVORO: VERSO LA REGOLAZIONE DEL *MANAGEMENT* ALGORITMICO*

Federica Palmirotta
Assegnista di ricerca in Diritto del Lavoro nell'Università degli Studi di Modena e Reggio Emilia

SOMMARIO: 1. Premessa. L'Intelligenza Artificiale e il *management* algoritmico: un mosaico normativo *in fieri*. - 2. L'ambito di applicazione del Regolamento IA. - 2.1. L'ambito di applicazione materiale. - 2.2. L'ambito di applicazione soggettivo. - 3. Le tecniche di tutela del Regolamento IA: *governance* dei rischi, trasparenza e rimedi. - 4. Riflessioni conclusive.

1. Premessa. Il Regolamento sull'Intelligenza Artificiale e il *management* algoritmico: un mosaico normativo *in fieri.*

Benché la nascita dell'Intelligenza Artificiale (d'ora in avanti, IA) si faccia generalmente risalire alla seconda metà del '900 e, nello specifico, in occasione della Conferenza di Darthmouth[64], è solo in tempi più recenti che quest'ultima ha avuto una diffusione pulviscolare ed ha invaso ogni settore produttivo e commerciale, introducendosi anche nella gestione del rapporto di lavoro.

Complice dell'inarrestabile successo della gestione algoritmica delle risorse umane, che spiega anche il trionfo, solo recente, della tecnologia dell'IA è l'accesso agevolato ai *Big Data* di cui, come è noto, l'IA si alimenta[65]. Gli stessi *Big Data* hanno anche causato una crescente digitalizzazione dei processi di gestione delle risorse umane, determinando il passaggio da funzioni principalmente amministrative a funzioni sempre più strategiche e specializzate, note con il nome di *People Analytics* o *management* algoritmico[66].

* Relazione al Seminario "Lavoro, impresa e nuove tecnologie dopo l'AI Act" svoltosi il 14 maggio 2024 presso la
Fondazione Biagi.

64 Nel 1956 il matematico John McCarthy propose di avviare un workshop estivo al Darthmount College dedicato allo studio dell'IA. Si veda MCCARTHY J. ET AL, *A proposal for the Darthmount Summer Research Project in Artificial Intelligence*, inviata alla Rockfeller Foundation e di cui rende notizia MITCHELL M., *Artificial Intelligence. A guide for thinking humans*, Londra, 2019.

65 Si veda ad es. BERSIN, J., *How Big Data tools helps HR understand you*, in *Forbes*, 29th February 2012, reperibile al link: https://www.forbes.com/sites/joshbersin/2012/02/29/how-bigdata-tools-helps-hr-understand-you/ (ultimo accesso 13 luglio 2024); DAVENPORT T. H., *Big data at work: Dispelling the myths, uncovering the opportunities*, Harvard Business Review Press, Boston, 2014; PHAN P., WRIGHT M., LEE S. H., *Of robots, artificial intelligence, and work*, in *The*
Academy of Management Perspectives, 31, 4, 2017, 253 255. Più recentemente, AGARWAL A., *AI adoption by human resource management: a study of its antecedents and impact on HR system effectiveness*, in *Foresight*, 25, 1, 2023, 67-71.

66 JOHNSON B.A.M., COGGBURN J. D., LLORENS J.J., *Artificial Intelligence and Public Human Resource Management: Questions for Research and Practice*, in *Public Personnel Management*, 51, 4, 2022, 538 562; RASMUSSEN T., ULRICH D.,

Difatti, l'elaborazione e l'analisi dei *Big Data* e l'implementazione di sistemi di AI nei processi HR ha permesso di sviluppare sistemi di *management* algoritmico che supportano o assumono decisioni organizzative, almeno in parola, più oggettive ed imparziali, in grado di incrementare la produttività della forza lavoro e ridurre i rischi di inaccuratezza.

Tuttavia, la letteratura ha ampiamente dimostrato che questo *trend* di digitalizzazione ha numerose implicazioni in termini giuslavoristici.[67] Tra le altre, la presunta imparzialità ed oggettività si dimostra in realtà solo apparente, in quanto risulta ormai appurato che gli algoritmi utilizzati nei sistemi di *management* hanno l'elevata probabilità di perpetuare o addirittura esacerbare i rischi di discriminazione, in virtù del loro impatto su larga scala. Più in generale, i sistemi di IA utilizzati nell'ambito del *management* algoritmico hanno la capacità di incidere direttamente sulle opportunità di accesso e in generale su ogni condizione di lavoro, in quanto le funzioni organizzative abilitate dall'IA ricoprono ogni aspetto della relazione lavorativa, dal reclutamento e selezione del personale alla risoluzione del rapporto di lavoro, dalla valutazione della performance, esercitata mediante nuovi strumenti di controllo ad alto contenuto tecnologico, tra cui ad esempio i dispositivi indossabili, alla pianificazione dei turni, da sistemi di IA utilizzati per suggerire percorsi formativi o nelle progressioni di carriera ai sistemi utilizzati per l'amministrazione dei compensi e degli altri benefici sino a sistemi utilizzati per ridurre il rischio di dimissioni e il rischio di fuga dei lavoratori[68].

L'esempio di applicazione dell'IA in ambito lavoristico più discusso in dottrina e con un'influenza nella determinazione (e nel deterioramento) delle condizioni lavorative concerne il lavoro su piattaforma. Quest'ultimo ha consegnato una chiara fotografia di come l'applicazione dell'IA nella gestione del rapporto di lavoro determini una tensione espansiva dei poteri datoriali a detrimento dei lavoratori[69]. Il tentativo del legislatore di contenere e regolare tale espansione ha reso il lavoro su piattaforma un autentico laboratorio normativo

Learning from practice: How HR analytics avoids being a management fad, in *Organizational Dynamics*, 44, 3, 2015, 236–242.

[67] Si vedano tra i numerosi riferimenti a riguardo, ICHINO P., *Subordinazione, autonomia e protezione del lavoro nella "gig-economy"*, in *Rivista Italiana di Diritto del Lavoro*, 2, 2018, 294–303; RECCHIA G. A., *Gig economy e dilemmi qualificatori: la prima sentenza italiana*, in *il Lavoro nella Giurisprudenza*, 7, 2018, 721–734.

[68] Per una definizione di *management* algoritmico, si vedano: GAUDIO G., *Algorithmic Bosses Can't Lie! How to Foster Transparency and Limit Abuses of the New Algorithmic Managers*, in *Comparative Labor Law & Policy Journal*, 42, 2022a, 707-741; PONCE DEL CASTILLO A., NARANJO D., *Regulating algorithmic management* , ETUI Policy Brief European Economic, Employment and Social Policy, August, 2022; WOOD A. J., *Algorithmic management consequences for work organisation and working conditions*, in *JRC Working Papers Series on Labour, Education and Technology*, No. 2021/07, European Commission, Joint Research Centre (JRC), Seville, 2021.

[69] Offrono una panoramica dei rischi del lavoro su piattaforma, tra gli altri, DE STEFANO V., *The Rise of the Just-in-Time Workforce: On-Demand Work, Crowdwork, and Labor Protection in the Gig-Economy*, in *Comparative Labor Law & Policy Journal*, 37, 3, 2015, 471-504; Aloisi A., *Commoditized Workers: Case Study Research on Labor Law Issues Arising from a Set of "On-Demand/Gig Economy" Platforms*, in *Comparative Labor Law & Policy Journal*, 37, 3, 2015, 653-689.

in area giuslavoristica in relazione ad un fenomeno i cui confini si sono progressivamente allargati nel mondo reale.

Tale inarrestabile diffusione, foriera di notevoli vantaggi e delicati rischi, ha giustificato l'attenzione del legislatore, europeo e nazionale, il quale, cercando di delineare un quadro regolatorio per la rivoluzione tecnologica in atto, è intervenuto con più atti legislativi che, a diverso livello e con una geometria di applicazione variabile, compongono oggi il complesso mosaico normativo del *management* algoritmico[70].

Il Regolamento IA, pubblicato in Gazzetta Ufficiale lo scorso 12 luglio[71], costituisce la tessera più recente che completa il mosaico, all'esito di un incessante impegno che negli ultimi anni la Commissione Europea ha dedicato al tema dell'IA e dei diritti fondamentali, dimostrato dai numerosi documenti ufficiali che precedono la Proposta di Regolamento dell'aprile 2021[72].

Si tratta, peraltro, di uno strumento legislativo peculiare ed orizzontale nell'ambito del sistema del diritto del lavoro, di fatti, benché, come si vedrà *infra*, costituisca una fonte generalista e non specialistica della materia giuslavoristica, esso produce un impatto non trascurabile nel sistema delle norme, delineando ad esempio alcuni obblighi a carico del datore di lavoro che intenda adottare un sistema di IA. Ciò è confermato dall'attenzione che la dottrina ha convogliato nell'analisi ad esso dedicata, sin dal momento in cui è stata proposto dalla Commissione Europea[73].

Delineato, quindi, il contesto di riferimento e considerato il ruolo che nell'immediato futuro rivestirà tale strumento legislativo nel sistema del diritto del lavoro, l'obiettivo del presente saggio è di ricostruire le tutele dei lavoratori e, contestualmente, gli obblighi dei

---

[70] CIUCCIOVINO S., *La disciplina nazionale sulll'utilizzazione dell'intelligenza artificiale nel rapporto di lavoro*, in *Lavoro Diritti Europa*, 1, 2024, parla di "deriva iperregolativa", che non necessariamente implica un incremento di tutele.
[71] Regolamento (UE) 2024/1689 del Parlamento Europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale).
[72] Tra gli altri, ad es.: la Comunicazione del 25 aprile 2018 "L'intelligenza artificiale per l'Europa", la Comunicazione 8 aprile 2019 "Creare fiducia nell'intelligenza artificiale antropocentrica"; i documenti prodotti dal gruppo di esperti ad alto livello sull'IA (AI HLEG); il Libro Bianco "sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia" del 19 febbraio 2020; fino ad arrivare il 21 aprile 2021 alla Proposta di Regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza Artificiale (Legge Sull'intelligenza Artificiale).
[73] Si citano ad esempio: ADAMS-PRASSL J., *Regulating algorithms at work: Lessons for a 'European approach to artificial intelligence'*, *in European Labour Law Journal*, 13, 1, 2022, 30-50; ALAIMO A., *Il Regolamento sull'Intelligenza Artificiale: dalla proposta della Commissione al testo approvato dal Parlamento. Ha ancora senso il pensiero pessimistico?*, in *Federalismi.it*, Focus Lavoro, Persona, Tecnologia 18 ottobre 2023; KELLY-LYTH A., *The AI Act and Algorithmic Management*, in *Comparative Labor Law & Policy Journal*, Dispatch no. 39, 2021, 6; PERUZZI M., *Intelligenza artificiale e lavoro. Uno studio su poteri datoriali e tecniche di tutela*, Giappichelli, Torino, 2023; PONCE DEL CASTILLO A., *The AI Regulation: entering an AI regulatory winter? Why an ad hoc directive on AI in employment is required*, European Trade Union Institute, 2021; VEALE M., BORGESIUS Z., *Demystifying the Draft EU Artificial Intelligence Act. Analysing the good, the bad, and the unclear elements of the proposed approach*, in *Computer Law Review International*, 4, 2021, 104.

datori di lavoro ai tempi del *management* algoritmico, così come modificati dall'avvento del Regolamento IA.

Nel perseguire tale obiettivo, l'indagine sarà preliminarmente dedicata allo studio e all'interpretazione del Regolamento, ponendolo in relazione, ove possibile, con gli altri strumenti regolatori che compongono il sostrato legislativo di riferimento, così da determinarne, innanzitutto, il confine di applicazione e, in secondo ordine, descrivere e sistematizzare le tecniche protettive adottate dal legislatore europeo al fine di definire gli adempimenti necessari per la *compliance*, anche in considerazione dell'eventuale interazione con le altre fonti.

Nello specifico, alcuni degli strumenti legislativi che saranno presi in considerazione in prospettiva integrata col Regolamento sono: a livello sovranazionale, il Regolamento sulla Protezione dei Dati Personali (Regolamento UE 2017/679), la Proposta di Direttiva del Parlamento Europeo e del Consiglio relativa al miglioramento delle condizioni di lavoro nel lavoro mediante piattaforme digitali (d'ora in avanti, Direttiva Piattaforme)[74] e, a livello nazionale, l'art. 4 dello Statuto dei Lavoratori, l'art. 1-bis D.lgs. n. 152/1997, il D. lgs. n. 25/2007.

2. L'ambito di applicazione del Regolamento IA.

Prima di procedere alla delimitazione dell'ambito materiale e soggettivo di applicazione del Regolamento, pare opportuno precisare, come già anticipato, che il Regolamento IA non adotta una base giuridica di matrice giuslavorista e, al contrario, si riferisce all'art. 114 TFUE, che esclude la diretta ricaduta migliorativa nel diritto del lavoro, e all'art. 16 TFUE, relativo invece alla tutela dei dati personali. Di conseguenza, in coerenza con la base giuridica di riferimento, gli obiettivi che lo strumento legislativo ambisce ad ottenere sono, da un lato, il miglioramento del funzionamento del mercato interno per lo sviluppo, l'immissione, la messa in servizio, e l'uso di sistemi di IA conformemente ai valori dell'UE; dall'altro, l'affidabilità, l'antropocentrismo e la garanzia del rispetto della salute, della sicurezza e diritti fondamentali sanciti nella CDFUE. Questa premessa, relativa alla base giuridica, deve costituire per lo studioso uno strumento di interpretazione giuridica teleologica, che non può essere ignorato nell'indagine delle norme.

Fatta questa premessa metodologica, nei sottoparagrafi seguenti si tenta di circoscrivere l'ambito di applicazione del Regolamento, con riguardo ai sistemi di *management* algoritmico.

[74] Il testo della Direttiva è stato ufficialmente adottato dal Parlamento Europeo lo scorso 24 aprile 2024 (reperibile al link: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0330_EN.html) e se ne attende ora la pubblicazione nella Gazzetta Ufficiale.

2.1. L'ambito di applicazione materiale.

Rispetto all'ambito di applicazione materiale, emerge un primo problema relativo all'ampiezza della fattispecie normativa. Difatti, il regolamento si riferisce espressamente a ciascun "sistema di IA automatizzato progettato per funzionare con livelli di autonomia variabile, che presenta adattabilità dopo la diffusione, che per obiettivi espliciti o impliciti, deduce dall'*input* che riceve come generare *output* quali previsioni, contenuti, raccomandazioni"[75]. Esaminando tale definizione congiuntamente al Considerando 12, al fine di qualificare un sistema come un sistema di IA, ai sensi del Regolamento, parrebbe essere necessaria la c.d. "capacità inferenziale"[76], vale a dire l'attitudine a dedurre risultati, quali raccomandazioni o pareri, o ricavare modelli e algoritmi, partendo dall'elaborazione e dall'analisi di dati e informazioni con cui l'IA è istruita. In queste caratteristiche si annoverano sia i sistemi costruiti con un approccio di autoapprendimento, sia sistemi, meno complessi, basati sulla logica e sulla conoscenza, che desumono, autonomamente, modelli a partire dalla conoscenza codificata. In sostanza, il regolamento fa propria la nota distinzione tra tecniche di *machine learning* (ML), caratterizzate dall'abilità di apprendere autonomamente dalle istruzioni fornite al fine di ottimizzare i risultati, e tecniche *knowledge-based*, qualificate generalmente dall'elevata comprensibilità, spiegabilità e prevedibilità del risultato, in quanto quest'ultimo giunge all'esito dell'applicazione di regole di inferenza ad una conoscenza codificata[77]. Non a caso, l'approccio deterministico di tali tecniche qualifica i sistemi di IA programmati con questa tecnica tendenzialmente "statici"[78].

Inoltre, lo stesso Considerando esclude dal novero di IA i sistemi basati su regole definite unicamente da persone fisiche per eseguire operazioni in modo automatico.

Pertanto, mentre la ricaduta nell'alveo del Regolamento è acclarata per i sistemi di IA programmati e addestrati con algoritmi di ML, i sistemi programmati con approccio *knowledge-based* pongono qualche problema interpretativo, da cui deriva anche la confusione, comune ai non esperti, tra le nozioni di IA, algoritmi e, in generale, sistemi automatizzati. Nello specifico, sarebbero qualificabili come sistemi di IA quelli programmati con approccio

[75] È questa la definizione di sistema di IA che il Regolamento restituisce all'art 3, par. 1, n.1.
[76] Il Considerando 12 parla in proposito di caratteristica *fondamentale* ai sistemi di IA.
[77] Occorre precisare a riguardo che il testo originale della Proposta di Regolamento IA aveva un contenuto più ristretto, in quanto individuava tassativamente le tecniche con cui il sistema di IA potesse svilupparsi, includendovi espressamente entrambe le tecniche. In particolare, l'art. 3, par. 1, punto 1, Proposta Regolamento IA definiva così il sistema di IA: "un software sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I, che può, per una determinata serie di obiettivi definiti dall'uomo, generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono."
[78] GERARDS J., XENIDIS R., *Algorithmic discrimination in Europe: Challenges and opportunities for gender equality and non-discrimination law*, Luxembourg: Publications Office of the European Union, 2021, 33.

knowledge-based che, a partire da regole d'inferenza e rapporti di condizionalità codificati in sede di programmazione, conservano la suddetta capacità inferenziale; al contrario, rimarrebbero esclusi i sistemi che operano in base a regole predefinite esclusivamente da persone fisiche per eseguire operazioni in modo automatico. Dunque, la linea di confine tra le due tipologie di sistema è estremamente sottile, senza contare poi che la distinzione è ulteriormente complicata dal noto problema della opacità caratterizzante l'IA e gli algoritmi[79].

In una logica di sistematizzazione delle fonti, resterebbe da chiedersi se dalla definizione di IA, risulti una sovrapposizione con la nozione di "trattamento automatizzato", utilizzata dal Regolamento sulla protezione dei dati personali, quella di "sistema decisionale o di monitoraggio automatizzato" adottata dalla Direttiva Piattaforme e assimilata anche dal legislatore nazionale nell'art. 1-bis del D. lgs. 152/1997 e, infine, quella più risalente, ma pur sempre attuale di "strumento di controllo a distanza", ex art. 4 St. Lav.

Rispetto alla nozione di "trattamento automatizzato" e "sistema decisionale o di monitoraggio automatizzato", ciò che appare scontato è che nel Regolamento IA il discrimine è sulla tecnica o sull'approccio di addestramento del sistema che deve essere tale da emulare le capacità decisionali umane. Viceversa, nel caso delle altre fonti, il legislatore sembra focalizzare la sua attenzione sulla destinazione d'uso o le caratteristiche del sistema o trattamento, sia essa la valutazione di aspetti personali relativi ad una persona fisica[80], ovvero il monitoraggio o la valutazione dell'esecuzione della prestazione lavorativa, ovvero l'uso finalizzato all'assunzione o al supporto di decisioni relative alle condizioni di lavoro[81]. Sul piano della tecnica, invece, in questa seconda fattispecie, sarà sufficiente la mera automatizzazione del processo o dell'insieme di regole predefinite, anche più basilare e non abilitata dall'IA.

In sintesi, la nozione di trattamento automatizzato o di sistema automatizzato è necessariamente più ampia, perché quest'ultima può essere svolta anche senza integrare nel

[79] Sulla complessità della linea di demarcazione che segna la soglia di ingresso nella nozione di IA, si veda PERUZZI M., *Sistemi automatizzati e tutela della salute e della sicurezza sul lavoro*, in *Diritto della Sicurezza sul Lavoro*, 2, 2024, 86.

[80] Ciò che per esempio accade nella profilazione, così come definita dall'art. 4, punto 4, del Regolamento sulla Protezione dei Dati Personali.

[81] Ad es. l'art. 2, par. 1, punto 9, Direttiva Piattaforme, definisce i sistemi decisionali automatizzati come "i sistemi utilizzati per prendere o sostenere, con mezzi elettronici, decisioni che incidono significativamente sulle persone che svolgono un lavoro mediante piattaforme digitali, tra cui le condizioni di lavoro dei lavoratori delle piattaforme digitali, in particolare decisioni che influenzano la loro assunzione, il loro accesso agli incarichi di lavoro e la relativa organizzazione, i loro guadagni, compresa la fissazione del prezzo dei singoli incarichi, la loro sicurezza e salute, il loro orario di lavoro, il loro accesso a formazione, promozione o suo equivalente, la loro situazione contrattuale, compresa la limitazione, la sospensione o la chiusura del loro account". Invece, l'art. 1-bis, D. lgs. n. 152/1997 si riferisce ai "sistemi decisionali o di monitoraggio integralmente automatizzati deputati a fornire indicazioni rilevanti ai fini della assunzione o del conferimento dell'incarico, della gestione o della cessazione del rapporto di lavoro, dell'assegnazione di compiti o mansioni nonché indicazioni incidenti sulla sorveglianza, la valutazione, le prestazioni e l'adempimento delle obbligazioni contrattuali dei lavoratori".

sistema una tecnica di IA.

Anche la nozione di "strumento di controllo a distanza" è più ampia e può includere quella di sistema di IA, laddove quest'ultimo è utilizzato con la finalità di monitorare il lavoratore. Trattasi, infatti, di uno strumento digitale ed elettronico che può anche implicare il controllo sull'attività del lavoratore. In detta circostanza, la fattispecie sarà sussumibile in quella disciplinata dall'art. 4 St. Lav, con tutte le conseguenze applicative che ne derivano[82].

Benché nella definizione di sistema di IA non siano rilevanti la destinazione o la finalità d'uso, queste ultime non sono completamente avulse dal Regolamento IA. Difatti, esse vengono prese in considerazione per valutare la rischiosità del sistema di IA, considerando tanto la potenzialità dell'impatto lesivo quanto la gravità dello stesso. Sulla scorta di tale valutazione il Regolamento gradua l'intensità delle norme da applicare. È quella qui descritta l'essenza dell'approccio basato sul rischio, su cui è incentrato l'intero impianto regolatorio del Regolamento, che, oltretutto, costituisce una tecnica di tutela già impiegata altrove nel diritto del lavoro[83].

A tal riguardo, il Regolamento distingue tra: *i)* rischi inaccettabili (Capo II, art. 5), *ii)* rischi elevati (Capo III), *iii)* finalità generali (Capo V).

Lungi dal qualificare nel dettaglio ognuna di queste categorie, ci si può limitare in questa sede ad individuare quelle che interessano il mondo del lavoro.

In proposito, si può già anticipare che nessun sistema di IA adottato nell'ambito del contesto lavorativo potrebbe essere considerato un sistema di IA per finalità generali, stante l'elevata pericolosità della violazione dei diritti dei lavoratori. Quest'ultima a volte integra un rischio inaccettabile da cui deriva il divieto di adottare tale pratica. Nello specifico, tra cui le pratiche vietate rientra la finalità di identificazione e inferenza delle emozioni dei lavoratori, fatta salva l'ipotesi in cui ciò serva per fini medici o di sicurezza[84]. Stante questa deroga, sarebbero in principio ammissibili sistemi che per motivi di sicurezza e, quindi, per rilevare un eventuale stato di affaticamento, stress, distrazione o dolore, catturino attraverso sensori e trattino informazioni sulla posizione e diametro della pupilla, sulla postura, sulla frequenza cardiaca e respiratoria, sulla temperatura corporea[85]. In questi casi, ferma restando la loro ammissibilità, rimarrà necessario attenersi agli altri obblighi previsti dall'ordinamento, per esempio in materia di trattamento dei dati personali e uso di processi decisionali automatizzati.

---

[82] Per approfondimenti si rimanda MARAZZA M., D'AVERSA F., *Dialoghi sulla fattispecie dei "sistemi decisionali o di monitoraggio automatizzati" nel rapporto di lavoro (a partire dal Decreto trasparenza)*, in *giustiziacivile.com*, 2022.
[83] Si pensi soprattutto alla normativa in materia di salute e sicurezza.
[84] Art. 5, punto f, Regolamento IA.
[85] Cfr. PERUZZI M., *op. cit.*

Altri esempi di rischio inaccettabile potrebbero essere connessi all'uso di sistemi categorizzazione biometrica per classificare le persone sulla base dei loro dati biometrici e trarre inferenze su dati sensibili, nonché all'uso di sistemi di valutazione e classificazione per assegnare un punteggio sociale alle persone da cui derivi un trattamento pregiudizievole o sfavorevole di persone fisiche o di interi gruppi in contesti sociali che non sono collegati ai contesti in cui i dati sono stati originariamente generati o raccolti.

In ogni caso, l'apporto significativo del Regolamento nell'area giuslavoristica rispetto alla regolazione del *management* algoritmico si ritrova nella disciplina applicata ai sistemi di IA ad alto rischio. Infatti, l'Allegato III del Regolamento individua alcuni ambiti tassativi nei quali, quindi, l'elevata rischiosità rispetto alla salute, alla sicurezza e ai diritti fondamentali derivante dall'uso del sistema di IA è qualificata *ex lege* e, dunque, presunta. Tra di essi si annoverano al punto 4 i sistemi di IA impiegati per finalità di "occupazione, gestione dei lavoratori e accesso al lavoro autonomo" nelle attività di reclutamento e selezione del personale, anche autonomo, e in ogni altra attività di gestione del rapporto di lavoro che impatti le condizioni lavorative[86]. Tale definizione, come è evidente, si sovrappone alla nozione di sistemi di *management* algoritmico. Di conseguenza, laddove tali sistemi siano sviluppati con tecniche di IA, dovranno essere conformi alla normativa prevista dal Regolamento relativa ai sistemi di IA ad alto rischio sia perché ne è riconosciuto l'impatto significativo sul futuro delle persone coinvolte, tanto in termini di prospettive di carriera quanto in termini di sostentamento e di diritti dei lavoratori, sia perché dal monitoraggio può derivare una violazione dei diritti fondamentali in materia di protezione dei dati personali.

Ferma restando la presunta elevata rischiosità di tali sistemi, l'art. 6, par. 3, del Regolamento ammette una deroga. Difatti, un sistema di IA potrebbe essere escluso dal novero dei sistemi ad alto rischio qualora non presenti un rischio significativo di danno per la salute, la sicurezza o i diritti fondamentali delle persone fisiche, ad esempio perché non influenza materialmente il risultato del processo decisionale. Si potrebbe, in via interpretativa, ipotizzare di escludere dall'area dei sistemi ad alto rischio quelli non "basat[i] unicamente" sul sistema automatizzato, per usare le parole del Regolamento sulla Protezione dei Dati Personali, che assicurino un coinvolgimento umano significativo tale per cui l'uomo conserva l'autonomia decisionale e il controllo della decisione algoritmica non si esaurisce in un

[86] Precisamente il punto 4, dell'Allegato III del regolamento si riferisce ai sistemi di IA destinati ad essere utilizzati: *i)* "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"; *ii)* "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."

semplice gesto simbolico[87].

In realtà, il Regolamento richiede, ai fini di applicazione della deroga, che sia soddisfatta una delle condizione tra: i) esecuzione di un compito procedurale limitato; ii) miglioramento del risultato di un'attività umana precedentemente completata; iii) rilevazione di schemi decisionali o deviazioni da schemi decisionali precedenti non finalizzata a sostituire o influenzare la valutazione umana precedente; iv) esecuzione di un compito preparatorio per una attività pertinente ai fini dell'allegato III.

Esiste, però, una clausola di salvaguardia: un sistema che effettua la profilazione delle persone fisiche, pur integrando una delle precedenti condizioni, sarà sempre qualificabile come sistema di IA ad alto rischio.

Per ciò che ivi riguarda, sembrerebbe difficile immaginare un sistema di *management* algoritmico che non implichi una valutazione di aspetti personali e non sia basata su dati personali, ossia due degli elementi caratterizzanti dell'attività di profilazione[88]. Ne dovrebbe conseguire che un sistema di *management* algoritmico, in linea di principio, sarà sempre qualificabile come un sistema ad alto rischio e sarà sempre tenuto a rispettare i requisiti per i sistemi ad alto rischio individuati nel Capo III, sez. 2[89].

2.2. L'ambito di applicazione soggettivo.

Avendo chiarito l'ambito di applicazione oggettivo del Regolamento con particolare riguardo agli aspetti che interessano la materia giuslavoristica, una delle conseguenze dell'approccio basato sul rischio è la puntuale identificazione del centro di imputazione degli obblighi e della responsabilità lungo l'intera filiera "digitale", tra cui ad esempio il soggetto importatore o il distributore.

I soggetti principali intorno a cui sono distribuiti gli obblighi della filiera "digitale" sono il fornitore e l'utilizzatore (definito dal Regolamento come *deployer*). Il primo è colui che sviluppa o fa sviluppare un sistema di IA ad alto rischio e lo immette sul mercato europeo o lo mette in servizio con il proprio nome o marchio, anche a titolo gratuito, e a prescindere

[87] GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, 6 febbraio 2018, 23.

[88] Si ricorda che, ai sensi dell'art. 4, punto 4, Regolamento sulla protezione dei dati personali, per profilazione si intende "qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica." Si vedano anche i commenti del GRUPPO DI LAVORO ARTICOLO 29, *op. cit.*, 7.

[89] Concordemente PERUZZI M., *op. cit.*, 2024, 88: "Considerato che quest'ultima condizione è molto probabile che si verifichi in caso di utilizzo di processi automatizzati di monitoraggio o decisionali sul lavoro, può ritenersi tendenzialmente da escludere una classificazione come "a basso rischio" dei sistemi destinati a essere utilizzati nell'esercizio di prerogative datoriali nei confronti dei lavoratori."

dalla sua collocazione geografica[90]. L'utilizzatore, invece, coincide con la persona fisica o giuridica, compresa un'autorità pubblica, un'agenzia o altro organismo, che utilizza il sistema di IA sotto la propria autorità per l'esercizio di un'attività professionale e non personale[91]. Come si vedrà *infra*, fornitore è il soggetto in capo al quale si configurano la maggior parte degli obblighi, tuttavia, in relazione ai sistemi di IA di *management* algoritmico, sarà più probabile che il datore di lavoro rivesta il ruolo di utilizzatore.

Il minor carico di responsabilità in capo al datore di lavoro è stato accolto criticamente da una parte della dottrina, che ne ha intravisto un tentativo di scaricare la responsabilità ad un soggetto terzo[92]. In realtà, come è stato anche sostenuto[93], la configurazione dell'obbligo in capo al soggetto che concretamente sviluppa e vende il sistema di IA non solo è coerente con la base giuridica e l'obiettivo del Regolamento di tutelare il mercato, ma assolve anche un'altra funzione di efficacia ed effettività: ciò sia perché il fornitore è un soggetto della filiera "digitale" che non può essere esente da responsabilità, considerato che sovente il datore di lavoro acquista il sistema di IA da soggetti terzi e lo integra nella propria organizzazione, sia perché, essendo lo sviluppatore del sistema, egli può concretamente disporre di esso, modificandone gli effetti e mitigandone l'impatto.

L'identificazione del fornitore nella filiera del sistema di IA è così necessaria che in alcuni casi si prescinde dal fatto la persona fisica o giuridica sia effettivamente lo sviluppatore del sistema. Difatti, il Regolamento identifica alcune condizioni specifiche in presenza delle quali, ai fini di certezza del diritto, qualsiasi soggetto della catena può essere considerato il fornitore del sistema di IA ad altro rischio e, pertanto, assumere tutti gli obblighi del caso[94].

Si tratta, nello specifico, di una delle seguenti ipotesi: i) l'utilizzatore apponga il proprio nome o marchio sul sistema di IA; ii) l'utilizzatore modifica in modo sostanziale il sistema di IA ad alto rischio, non mutandone le caratteristiche che lo rendono tale; iii) l'utilizzatore modifica un sistema per finalità generale rendendolo ad alto rischio[95].

Considerata la rilevanza della "qualificazione" soggettiva, da cui discende il centro di imputazione delle principali responsabilità, e considerato il fatto che, come detto, nei sistemi di IA di *management* algoritmico il datore di lavoro coincide spesso con l'utilizzatore, è legittimo chiedersi quali siano i requisiti che rendono una modifica al sistema "sostanziale".

[90] Art. 3, punto 3, Regolamento IA.
[91] Art. 3, punto 4, Regolamento IA.
[92] DE STEFANO V., WOUTERS M., *AI and digital tools in workplace management and evaluation: An assessment of the EU's legal framework*, STOA: Panel for the Future of Science and Technology, Brussels, European Union, 2022, 55; VEALE M., BORGESIUS Z., *op. cit.*
[93] KELLY-LYTH A., *op. cit.*
[94] Considerando 84, Regolamento IA.
[95] Art. 25, par. 1, Regolamento IA.

A supporto dell'interpretazione di questo concetto intervengono l'art. 3, punto 23, e il Considerando 128, i quali chiariscono che non rientrano in questo confine le modifiche che sono naturale conseguenza della capacità di apprendimento del sistema a partire dai dati che riceve, purché siano state predeterminate dal fornitore e valutate al momento della valutazione di conformità richiesta dal Regolamento[96] [97].

In ogni caso, anche qualora l'utilizzatore modificasse sostanzialmente il sistema di IA ad alto rischio, il fornitore originario conserverebbe l'obbligo di cooperare al fine di consentire all'utilizzatore-fornitore di adempiere i suoi obblighi.

3. Le tecniche di tutela del Regolamento IA: *governance* dei rischi, trasparenza e rimedi.

Le tecniche di tutela individuate dal Regolamento IA si ispirano ai sette requisiti etici fondamentali che i sistemi di IA dovrebbero rispettare per essere affidabili, ossia: intervento e sorveglianza umani; robustezza tecnica e sicurezza; vita privata e *governance* dei dati; trasparenza; diversità, non discriminazione ed equità; benessere sociale e ambientale; responsabilità[98]. Tali requisiti, come si vedrà, costituiscono il nucleo minimo di garanzie che ciascun sistema di IA implementato in ambiti che integrano un rischio elevato sono tenuti a rispettare. Nello specifico, i requisiti chiave trovano una sistematizzazione nel Regolamento al Capo III, nella sez. 2, dedicata ai "Requisiti per i sistemi ad alto rischio", che elenca gli elementi necessari per un sistema di IA conforme al Regolamento, e nella sez. 3 intitolata "Obblighi dei fornitori e dei *deployer* dei sistemi di IA ad alto rischio e di altre parti", che, invece, si occupa di distribuire le responsabilità tra i soggetti coinvolti.

L'applicazione di tali tecniche di tutela al contesto lavorativo evidenzia, peraltro, il nuovo *trend* di regolazione che il diritto del lavoro sta sperimentando, in base al quale a strumenti regolatori di tipo prescrittivo-rimediale si aggiungono strumenti di natura preventiva e

[96] Considerando n. 128, Regolamento IA: "Tuttavia, le modifiche apportate all'algoritmo e alle prestazioni dei sistemi di IA che proseguono il loro "apprendimento" dopo essere stati immessi sul mercato o messi in servizio, in particolare adattando automaticamente le modalità di svolgimento delle funzioni, non dovrebbero costituire una modifica sostanziale, a condizione che tali modifiche siano state predeterminate dal fornitore e valutate al momento della valutazione della conformità". L'art. 3, punto 23, invece, definisce la "modifica sostanziale", come "modifica di un sistema di IA a seguito della sua immissione sul mercato o messa in servizio che non è prevista o programmata nella valutazione iniziale della conformità effettuata dal fornitore e che ha l'effetto di incidere sulla conformità del sistema di IA ai requisiti di cui al capo III, sezione 2, o comporta una modifica della finalità prevista per la quale il sistema di IA è stato valutato".

[97] L'eventuale redistribuzione degli obblighi conseguente alla modifica sostanziale pone anche problemi in termini di sostenibilità degli oneri che potrebbero essere troppo gravosi per le PMI. Sul tema si vedano i contributi di PALLADINI V. e CICCIA ROMITO C., in questo volume.

[98] Si tratta dei sette requisiti individuati dall'AI HLEG, in *Etichs guidelines for trustworthy AI*, reperibile in: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.

promozionale[99].

Provando a riassumere gli strumenti protettivi, se ne ricavano tre macro-approcci regolativi, tra loro strettamente interconnessi: il primo orientato alla *governance* del rischio; il secondo teso alla promozione della trasparenza; e il terzo relativo agli strumenti correttivi e rimediali.

Rispetto alla *governance* del rischio, numerosi referenti normativi convergono in questa direzione.

In primo ordine, ai sensi dell'art. 9, il fornitore deve adottare un sistema di gestione del rischio. Trattasi, nello specifico, di un processo iterativo, che richiede un aggiornamento costante e sistematico. Tale sistema si compone di varie fasi: innanzitutto, l'identificazione e la valutazione dei rischi noti e ragionevolmente prevedibili in condizioni di corretto utilizzo in materia salute, sicurezza e diritti fondamentali nonché di quelli che potrebbero emergere in caso di un uso improprio, ferma restando la loro ragionevole prevedibilità; la valutazione degli altri eventuali rischi che emergono *ex post* dai sistemi di monitoraggio; l'adozione di misure di gestione e correzione che siano opportune e mirate ai rischi così individuati. Si tratta, in sostanza, di realizzare una impalcatura di procedimentalizzazione dei rischi, sul modello della normativa in materia di salute e sicurezza sul lavoro[100]. La differenza in questo caso è che il soggetto responsabile di tale impalcatura è il fornitore, che, come detto, spesso non coincide con il datore di lavoro. Tuttavia, il datore di lavoro, in quanto utilizzatore, sarà informato su gli aspetti di tale sistema di gestione, che potranno essere particolarmente utili, in un momento successivo, per l'adempimento degli obblighi di SSL a suo carico. *A fortiori*, nell'ipotesi in cui il datore di lavoro personifichi il fornitore, perché ha modificato sostanzialmente il sistema, il sistema di gestione così definito diverrà presumibilmente parte integrante dell'obbligo prevenzionistico e agirà, quindi, anche come strumento di amplificazione delle tutele collettive[101].

In ogni caso, il requisito della ragionevole prevedibilità, così come quello relativo alla identificazione di una soluzione "tecnicamente possibile"[102], ricavabile dall'art. 9, par. 5, se

[99] Vedi sul punto, SENATORI I. in questo volume.

[100] Si pensi ad esempio alla Direttiva quadro sulla Salute e la Sicurezza sul Lavoro (SSL) (Direttiva 89/391/CEE), recepita nel nostro ordinamento insieme alle altre direttive in materia di SSL dal D.lgs. n. 81/2008.

[101] Di questa opinione PERUZZI M., *op. cit,*, 2024, 91.

[102] Nello specifico, l'art. 9, par. 5, Regolamento IA, richiede l'eliminazione o la riduzione del rischio "per quanto possibile dal punto di vista tecnico". Tale principio si sovrappone al principio nazionale della "massima sicurezza tecnologicamente possibile" applicato in materia di SSL ai sensi dell'art. 2087 c.c., e caratterizzante il modello di prevenzione italiano. Per approfondimenti, si vedano, fra gli altri, NATULLO G., *Principi generali della prevenzione e "confini" dell'obbligo di sicurezza*, in RUSCIANO M., NATULLO G. (a cura di), *Ambiente e sicurezza del lavoro*, Utet Giuridica, Segrate, 2008; cfr. anche, BALANDI G.G., *Individuale e collettivo nella tutela della salute nei luoghi di lavoro:l'art.9 dello Statuto*, in *Lavoro e Diritto*, 1990, 219 ss e ID.., *Il contenuto dell'obbligo di sicurezza*, in AA.VV.,

da una parte, restringono notevolmente il confine della responsabilità[103], dall'altra, comunque, potrebbero servire ad evitare che il soggetto sviluppatore o l'eventuale datore di lavoro debbano assumersi rischi potenzialmente *abnormi*, che fuoriescono dalla governabilità, cui si è cercato di rimediare anche mediante la preventiva consultazione di esperti e portatori di interessi[104].

Rientrano nel sistema di *governance* del rischio anche le altre norme che, ispirandosi al requisito della "robustezza tecnica", richiedono la conservazione della documentazione tecnica ai fini della conformità (art. 11), la capacità di registrazione (art. 12); la garanzia di accuratezza, robustezza e cibersicurezza (art. 15); la qualità e l'accuratezza dei dati (art. 10).

Quest'ultima è finalizzata anche ad evitare la potenziale riproduzione e diffusione su larga scala delle distorsioni, ossia i cd. *bias*, causate della non rappresentatività dei dati ovvero dall'uso di dati di addestramento non depurati dai pregiudizi sociali, istituzionali e storici[105]. A tal fine, il Regolamento richiede anche la predisposizione di misure atte a prevenire e correggere *attivamente* tali distorsioni[106].

Per un coordinamento con le altre fonti, si precisa che, rispetto alla garanzia di qualità dei dati, già il Regolamento sulla Protezione dei Dati personali interveniva sul punto, attraverso il principio di accuratezza. In questo caso, tuttavia, la differenza risiede nella maggiore ampiezza dell'ambito applicativo del Regolamento IA, in quanto non sarà necessaria ai fini dell'applicazione la "personalità" del dato di addestramento fornito al sistema di IA[107]. Al contrario, il Regolamento IA identifica una peculiare ipotesi di deroga all'uso dei dati sensibili,

---

L'obbligazione di sicurezza, in *Quaderni di Diritto del Lavoro e delle Relazioni Industriali*, Torino, 1994, 79 ss.

103 Della stessa opinione, CEFALIELLO A., KULLMANN M., *Offering false security: How the draft artificial intelligence act undermines fundamental workers rights*, in *European Labour Law Journal*, 2022, 13, 4, 542 ss., e PONCE DEL CASTILLO A., *op. cit.*

104 Considerando 65, Regolamento AI, "Il sistema di gestione dei rischi dovrebbe adottare le misure di gestione dei rischi più appropriate alla luce dello stato dell'arte in materia di IA. Nell'individuare le misure di gestione dei rischi più appropriate, il fornitore dovrebbe documentare e spiegare le scelte effettuate e, se del caso, coinvolgere esperti e portatori di interessi esterni. Nell'individuare l'uso improprio ragionevolmente prevedibile dei sistemi di IA ad alto rischio, il fornitore dovrebbe contemplare gli usi di sistemi di IA che, pur non essendo direttamente coperti dalla finalità prevista e considerati nelle istruzioni per l'uso, si può ragionevolmente prevedere derivino da un comportamento umano facilmente prevedibile nel contesto delle caratteristiche e dell'uso specifici di un determinato sistema di IA."

105 Per un approfondimento sull'incidenza dei *bias* e per una loro classificazione si vedano, tra gli altri: SCHWARTZ R., VASSILEV A., GREENE K., PERINE L., BURT A., *Towards a Standard for Identifying and Managing Bias in Artificial Intelligence*, NIST Special Publication 1270, 2022, 3; DANKS D., LONDON A., *Algorithmic bias in autonomous systems*, Proc. IJCAI, 2017, 4691–4697; FRIEDMAN B., NISSENBAUM H., *Bias in computer systems*, in *ACM Transactions on Information Systems*, 14, 3, 1996, 330–347.

106 Il riferimento legittimerebbe le tecniche di *debiasing*, note anche con il nome di "azioni positive algoritmiche", di cui in una prospettiva giuridica parlano ad esempio: BAROCAS S., SELBST A.D., *Big Data's Disparate Impact*, in *California Law Review*, 104, 2017, 705; BENT J.R., *Is Algorithmic Affirmative Action Legal?*, in *The Georgetown Law Journal*, 2019, 814.

107 FINOCCHIARO G., GRECO L., *Il ruolo di titolare, responsabile e contitolare del trattamento nei trattamenti i dati personali mediante intelligenza artificiale*, in PAJNO A., DONATI F., PERRUCCI F. (a cura di), *Intelligenza Artificiale e Diritto: una rivoluzione?*, Il Mulino, Bologna, 2022, 322.

regolato dall'art. 9 del Regolamento sulla Protezione dei Dati Personali. Difatti, esso è espressamente ammesso laddove sia strettamente necessario ai fini della rilevazione e della correzione delle distorsioni, benché ne sia condizionato l'uso al rispetto di una lista tassativa e concorrente di requisiti[108]. Si tratta, di fatto, di una questione di interesse pubblico rilevante, come anche chiarito dal Considerando 70, che sarebbe già tutelata dall' Art. 9, par. 2, lett. g), Regolamento sulla Protezione dei Dati Personali.

Quelli sin qui descritti sono oneri a carico del fornitore e, dunque, non rientrerebbero generalmente nella responsabilità del datore di lavoro. Tuttavia, nel novero degli strumenti di *governance* del rischio, deve essere inclusa anche la garanzia della sorveglianza umana (art. 14), finalizzata a prevenire i rischi per la salute, la sicurezza e i diritti fondamentali mediante il monitoraggio del funzionamento, di cui deve occuparsi prevalentemente il datore di lavoro, in qualità di utilizzatore del sistema. Egli, in ogni caso, deve essere previamente posto nelle condizioni di attuare tale sorveglianza attraverso istruzioni che rendano comprensibili, tra le altre, le capacità e i limiti del sistema, permettano di interpretare correttamente l'esito della decisione automatizzata ed eventualmente discostarsi da essa, nonché di interrompere e arrestare il sistema in caso di necessità. Al fine di consentire ai dipendenti deputati alla sorveglianza di assumere decisioni informate, il corollario dell'obbligo di sorveglianza umana è la necessità di fornire ai lavoratori, un livello adeguato di alfabetizzazione digitale, nonché la formazione e l'autorità in materia di IA per svolgere adeguatamente tali compiti[109].

Per quanto riguarda gli strumenti di promozione della trasparenza, le nuove tecniche di tutela impiegate nel diritto del lavoro graduano la trasparenza in due diverse livelli: innanzitutto, la trasparenza intesa come trasmissione di informazioni e strumento di acquisizione di consapevolezza *ex ante*; in secondo luogo, la trasparenza declinata come

[108] Art. 10, par. 5, Regolamento IA:
"a) il rilevamento e la correzione delle distorsioni non possono essere realizzati efficacemente mediante il trattamento di altri dati, compresi i dati sintetici o anonimizzati; b) le categorie particolari di dati personali sono soggette a limitazioni tecniche relative al riutilizzo dei dati personali, nonché a misure più avanzate di sicurezza e di tutela della vita privata, compresa la pseudonimizzazione;
c) le categorie particolari di dati personali sono soggette a misure tese a garantire che i dati personali trattati siano resi sicuri e protetti nonché soggetti a garanzie adeguate, ivi compresi controlli e documentazione rigorosi dell'accesso, al fine di evitare abusi e garantire che solo le persone autorizzate e sottostanti a opportuni obblighi di riservatezza abbiano accesso a tali dati personali;
d) le categorie particolari di dati personali non devono essere trasmesse, trasferite o altrimenti consultate da terzi;
e) le categorie particolari di dati personali vengono cancellate dopo che la distorsione è stata corretta oppure i dati personali hanno raggiunto la fine del loro periodo di conservazione, a seconda di quale delle due condizioni si verifica per prima;
f) i registri delle attività di trattamento a norma dei regolamenti (UE) 2016/679 e (UE) 2018/1725 e della direttiva (UE) 2016/680 comprendono i motivi per cui il trattamento delle categorie particolari di dati personali era strettamente necessario per rilevare e correggere distorsioni e i motivi per cui tale obiettivo non poteva essere raggiunto mediante il trattamento di altri dati."
[109] Art. 4, Regolamento IA.

misurazione e monitoraggio finalizzati al controllo *ex post*[110].

Rispetto alla prima forma di trasparenza, il Regolamento IA coinvolge diversi livelli e soggetti.

Innanzitutto, la trasmissione delle informazioni investe il flusso dal fornitore all'utilizzatore-datore di lavoro (art. 13), in modo da consentire di attuare concretamente ed efficacemente la sorveglianza umana e sì da conferire una tracciabilità "leggibile" alla decisione acquisita mediante il sistema di IA. Tali informazioni riguardano, ad esempio, le capacità e le caratteristiche tecniche per assolvere la richiesta di spiegazioni, di cui si dirà nell'analisi del terzo macro-approccio regolativo, nonché ogni informazione relativa alla manutenzione e alla cura del sistema.

Si aggiunge, poi, la trasparenza a cui è obbligato l'utilizzatore nei confronti dei portatori di interesse, variamente coinvolti (art. 26 e Considerando 93). Essa è particolarmente rilevante nell'ambito giuslavoristico perché sostanzia un diritto, minimo e necessario, di informazione dei lavoratori nei confronti del datore di lavoro che intenda adottare un sistema di gestione delle risorse umane integrando l'IA e, dunque, prima che essi siano soggetti al sistema. Nello specifico, questa forma di trasmissione di informazioni potrà avere come soggetti destinatari non solo i singoli lavoratori individualmente coinvolti, ma anche le rappresentanze dei lavoratori. Il coinvolgimento di queste ultime mediante forme di informazione collettiva, come è stato anche evidenziato anche in dottrina, consente un equilibrio più bilanciato rispetto all'espansione dei poteri datoriali[111].

Vieppiù, questo diritto minimo di informazione diverrebbe un autentico strumento partecipativo, laddove l'oggetto della informazione rientri nell'ambito applicativo definito dalle fonti, nazionali e sovranazionali, in materia di informazione e consultazione[112]. Il riferimento immediato a riguardo è alla Direttiva 2002/14/CE, recepita dal D. lgs. n. 25/2007, che, tuttavia, già innescava l'obbligo di avviare la procedura di informazione e consultazione in caso l'impresa adottasse "decisioni […] suscettibili di comportare rilevanti cambiamenti dell'organizzazione del lavoro". La decisione di adottare un sistema di IA per la gestione del rapporto di lavoro, indubbiamente, rientrerebbe in questo ambito.

In definitiva, il Regolamento IA, piuttosto che allargare o intensificare la garanzia del diritto di informazione e consultazione già regolamentato, si limita a confermarne l'applicazione anche all'ipotesi di introduzione di un sistema di IA di *management* algoritmico

[110] CIUCCIOVINO S., *op. cit.*, 14.
[111] *Ibidem.* Cfr anche i contributi di SENATORI I. e PURIFICATO I., in questo volume.
[112] L'art. 26, par. 7, Regolamento IA, infatti, precisa che "Tali informazioni sono fornite, se del caso, 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 ad estenderlo nei limitati casi in cui esso non fosse già tutelato dalle precedenti norme. Tra questi ultimi rientrano il caso in cui ad essere assoggettati al sistema di IA vi siano dei lavoratori autonomi, l'ipotesi in cui il numero complessivo dei dipendenti sia inferiore alla soglia dimensionale richiesta dalla Direttiva, ovvero nei confronti dei candidati che si trovano nella fase di selezione e reclutamento, che precede l'assunzione[113].

Bisogna precisare che nel nostro ordinamento questo diritto di informazione minima trova già un referente normativo nell'art. 1-bis, D. lgs. n. 152/1997, così come modificato dal Decreto Trasparenza, che espressamente obbliga i datori di lavoro a "informare il lavoratore [e le rappresentanze sindacali aziendali, ovvero la rappresentanza sindacale unitaria e, in assenza delle predette rappresentanze, le sedi territoriali delle associazioni sindacali comparativamente più rappresentative sul piano nazionale] dell'utilizzo di sistemi decisionali o di monitoraggio integralmente automatizzati deputati a fornire indicazioni rilevanti ai fini della assunzione o del conferimento dell'incarico, della gestione o della cessazione del rapporto di lavoro, dell'assegnazione di compiti o mansioni nonché indicazioni incidenti sulla sorveglianza, la valutazione, le prestazioni e l'adempimento delle obbligazioni contrattuali dei lavoratori"[114]. Richiamando quanto si è detto *supra* con riguardo all'ambito applicativo di tale disposizione, se ne deduce che essa troverà applicazione ogni qual volta il datore di lavoro adotti un sistema di *management* algoritmico, a prescindere che esso sia sviluppato o meno con tecniche di IA[115]. Ciò, del resto, trova anche conferma nel Disegno di Legge recante disposizioni e delega al governo in materia di intelligenza artificiale, che ai sensi dell'art. 10 impone al datore di lavoro o al committente di informare il lavoratore dell'utilizzo dell'intelligenza artificiale nei casi e con le modalità di cui all'articolo 1-bis del decreto legislativo 26 maggio 1997, n. 152"[116]. Si ritiene necessario evidenziare che tale formulazione non rispetterebbe quanto disposto dal Regolamento, in quanto richiama ai fini dell'informazione ai lavoratori unicamente la procedura ex art. 1-bis, D. lgs. n. 152/1997.

In merito, poi, all'oggetto di detta informazione, esso concerne unicamente la decisione di assoggettare i lavoratori all'uso del sistema di IA. Una tale informazione, piuttosto che

[113] Per un apprendimento sulla dimensione collettiva del diritto di informazione e l'apporto del Regolamento IA, si vedano i contributi di SENATORI I. e PURIFICATO I., in questo volume.

[114] Cfr. in commento alla normativa, ad esempio: RECCHIA G.A., *Condizioni di lavoro trasparenti, prevedibili e giustiziabili: quando il diritto di informazione sui sistemi automatizzati diventa uno strumento di tutela collettiva*, in *Labour & Law Issues*, 19, 1, 2023; 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*, 1, 2023, 7-40, e per un approccio più critico: FAIOLI M*., Trasparenza e monitoraggio digitale. Perché abbiamo smesso di capire la norma sociale europea*, in *Federalismi.it*, 25, 2022, 104-115.

[115] Per un approfondimento sui diritti di informazione nel Regolamento IA, nella disciplina nazionale, così come nelle altre fonti legislative, si veda il contributo di PURIFICATO I., in questo volume.

[116] Il testo del Disegno di Legge reperibile al seguente link: https://www.senato.it/service/PDF/PDFServer/DF/437373.pdf.

riguardare l'esito o gli effetti della decisione,[117] si limita ad assicurare un "controllo", comunque parziale, sul solo assoggettamento al sistema di IA e non sui rischi ad esso connessi.

Tale controllo rimarrebbe parziale in quanto si limita a delineare una mera garanzia di informazione *ex ante* sull'uso del sistema nella cui scelta il sindacato non potrà esercitare alcuna influenza. Ciò a differenza della proposta di Regolamento IA emendata dal Parlamento che prevedeva una partecipazione cd. "forte" in quanto si spingeva sino ad obbligare le parti a trovare un accordo [118] .

Per quanto riguarda la seconda forma di trasparenza, si include in tale categoria ogni procedura che consenta di scomporre il processo decisionale e soprattutto di valutarne gli esiti e gli effetti al fine di controllare e correggere gli eventuali abusi del ragionamento "artificiale"[119].

Anche rispetto a questa forma di trasparenza si evidenziano criticità in termini di efficacia, specie rispetto al confronto con altri strumenti legislativi, anche contigui, come la Direttiva Piattaforme.

Nello specifico, questa forma di trasparenza è strettamente legata al sistema di *governance* dei rischi, di cui si è parlato *supra* e, per il quale, come si è detto, è necessario fornire all'utilizzatore tutti gli strumenti idonei per procedere al monitoraggio. Ciò al fine di verificare che, nel concreto utilizzo del sistema di IA, non si realizzino rischi e violazioni dei diritti dei lavoratori. Per realizzare efficacemente questo sistema di prevenzione del rischio, è posto a carico dell'utilizzatore un onere di monitoraggio attivo, sia sulla pertinenza e rappresentatività dei dati,[120], sia sul funzionamento del sistema[121]. In questo secondo caso, possono configurarsi due distinte ipotesi che innescano l'attivazione di un obbligo di segnalazione a carico dell'utilizzatore: in presenza di un rischio per la salute, la sicurezza o per i diritti fondamentali delle persone, l'utilizzatore è tenuto ad informare, senza ritardo, il fornitore e gli altri soggetti della catena; qualora invece si verifichi un incidente grave, l'informazione al fornitore deve essere fornita in via immediata[122]. Si attiva, quindi, un sistema circolare di gestione del rischio nel quale, tuttavia, manca una qualsiasi forma di coinvolgimento per le rappresentanze dei lavoratori.

L'unica eccezione risiede nella valutazione di impatto sui di diritti fondamentali richiesta

[117] Rispetto all'importanza delle informazioni a consuntivo, vedi CIUCCIOVINO S., *op. cit.*
[118] Art. 29, par. 5bis, Proposta Regolamento IA (IMCO-LIBE), disponibile al seguente link: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_IT.html
[119] Cfr. nt. (53)
[120] Art. 26, par. 4, Regolamento IA.
[121] Art. 26, par. 5, Regolamento IA.
[122] Art. 26, par. 5, Regolamento IA.

ai sensi dell'art. 27 che spetta specificamente a determinati soggetti utilizzatori e per il cui svolgimento si potrebbe configurare un coinvolgimento dei portatori di interesse e dei loro rappresentanti[123]. Trattasi comunque di un obbligo che non compete agli utilizzatori di sistemi di *management* algoritmico, in quanto limitata ai soli utilizzatori che siano organismi di diritto pubblico o enti privati che forniscono servizi pubblici e impiegano sistemi di IA per l'accesso a servizi privati essenziali e a prestazioni e servizi pubblici essenziali e fruizione degli stessi.

Ne consegue un *deficit* di tutela rispetto alle disposizioni di altri referenti normativi. Infatti, già l'art. 35, del Regolamento sulla Protezione dei Dati Personali ammette una, pur lievissima, forma di coinvolgimento delle parti sociali per la redazione della valutazione di impatto sulla protezione dei dati. Quest'ultima, però, più che costituire uno strumento trasparenza-monitoraggio *ex post*, delinea una procedura per la gestione dei rischi *ex ante*.

La vera novità sul tema è rappresentata dalla disciplina della Direttiva Piattaforme, laddove le rappresentanze dei lavoratori assumono un ruolo di guardiano sia a monte che a valle del trattamento automatizzato, in quanto è previsto il loro coinvolgimento esplicito nella fase di valutazione dell'impatto delle decisioni. Quest'ultima deve avere cadenza almeno biennale, sì da consentire una verifica e un controllo concreti lungo il ciclo di vita del sistema algoritmico, che potenzialmente può spingersi sino alla necessità di modificare o cessare l'uso del sistema, laddove emerga una violazione dei diritti dei lavoratori su piattaforma ma soprattutto un elevato rischio di discriminazione[124].

Il terzo ed ultimo nucleo di norme che si ritengono rilevanti in questa indagine sono quelle relative agli strumenti correttivi e rimediali.

A tal riguardo, si annoverano le misure correttive disciplinate dall'art. 20 per rendere conforme il sistema di IA che non risponda ai requisiti di conformità, o eventualmente disabilitarlo, ritirarlo o richiamarlo dal mercato, tutte misure che sono appannaggio del solo fornitore. Tra gli strumenti correttivi, si fa rientrare anche la procedura che si attiva in caso di incidente grave, ad esempio la violazione degli obblighi posti a tutela dei diritti fondamentali. In tale circostanza, oltre a segnalare l'incidente all'autorità di vigilanza del mercato, il fornitore sarà anche tenuto a svolgere indagini per valutare il rischio dell'incidente e per individuare le necessarie misure correttive.

Infine, tra gli strumenti rimediali si annoverano, oltre al riscorso giurisdizionale, la possibilità per la singola persona fisica di presentare reclamo all'autorità di vigilanza[125], e

[123] Considerando 95, Regolamento IA.
[124] Art. 10, Direttiva Piattaforme.
[125] Art. 85, Regolamento IA.

specialmente il suo diritto alla spiegazione[126]. Si tratta di un diritto che ciascuna persona e lavoratore interessato, oggetto di una decisione che abbia effetti legali o incida significativamente nei suoi confronti, può esercitare al fine di ricevere spiegazioni chiare e significative dall'utilizzatore (e quindi dal datore di lavoro) sul ruolo del sistema di IA nella procedura decisionale e sui principali elementi della decisione adottata. Tale diritto sostanzierebbe il controllo *ex post*, di cui si diceva pocanzi, ma presenta almeno due limiti: innanzitutto, manca la possibilità di contestare direttamente la spiegazione, quando non soddisfacente, ed eventualmente richiedere la modifica della decisione[127]; inoltre, parimenti agli altri strumenti rimediali ivi considerati, esclude l'esercizio del diritto da parte dei rappresentanti dei lavoratori, avendo natura prettamente individuale. Si segnala, a riguardo, che anche questo limite del Regolamento IA sembrerebbe superato dalla Direttiva Piattaforme, che, da una parte, legittima il lavoratore su piattaforma e il suo rappresentante sindacale a chiedere il riesame della decisione e, dall'altra, invita gli Stati Membri a predisporre strumenti processuali collettivi aperti all'azione dei rappresentanti dell'interesse leso[128].

4. Riflessioni conclusive.

Il quadro normativo che l'UE ha predisposto a presidio del *management* algoritmico mediante il Regolamento IA risulta vischioso e pregno di criticità. Ciò che appare evidente è che il legislatore europeo volesse puntare su un modello disciplinare multilivello ispirato al principio della sussidiarietà, in cui l'intervento legislativo coinvolge anche la responsabilità dell'autonomia privata[129].

Le criticità rilevate rispetto alla tutela giuslavoristica sono numerose, fra tutte, si evidenziano la predisposizione di obblighi principalmente a carico del fornitore e non del datore di lavoro, così come anche la presenza di strumenti correttivi che, pure, sono preliminarmente appannaggio del fornitore, nonché la carente dimensione collettiva. Quest'ultima si configura quale grande assente della normativa in esame, stante anche l'orientamento prevalente in dottrina di dare impulso agli strumenti di partecipazione collettiva per la tutela dei nuovi rischi posti dall'uso delle nuove tecnologie[130].

---

126 Art. 86, Regolamento IA.
127 Si veda ALAIMO A., *op. cit.*
128 Art. 19, Direttiva Piattaforme.
129 VINCENZO PONTE F., *Intelligenza artificiale e lavoro. Organizzazione algoritmica, profili gestionali, effetti sostitutivi*, Giappichelli, Torino, 2024, 30.
130 Cfr. ad esempio: DE STEFANO V., *"Negotiating the Algorithm": Automation, Artificial Intelligence and Labor Protection*, in *Comparative Labor Law & Policy Journal*, 41, 2019, 15-32; ID., "*Masters and servers": Collective labour rights and private government in the contemporary world of work*, in *IJCLLIR*, 36, 4, 2020, 435–443; TODOLÍ-SIGNES A., *Algorithms, Artificial Intelligence and Automated Decisions Concerning Workers and the Risks of Discrimination: The Necessary Collective Governance of Data Protection*, in *Transfer: European Review of Labour and Research*, 25, 2019, 465; DAGNINO

Ad ogni modo, occorrerebbe domandarsi se avrebbe dovuto essere il Regolamento IA a farsi carico delle specificità del diritto del lavoro, o se, piuttosto, queste ultime dovessero essere demandate ad uno strumento *ad hoc*[131]. Non si deve dimenticare, infatti, che il Regolamento rimane una norma intersettoriale e non lavoristica, tesa anzi a tutelare espressamente il mercato unico.

Lungi dall'assumere una posizione acritica nei confronti del legislatore europeo, si ritiene di evidenziare che la Direttiva Piattaforme avrebbe potuto costituire proprio quello strumento *ad hoc* capace di tutelare i lavoratori vittima del "selvaggio" uso dell'IA nella gestione del rapporto lavorativo, se fosse andata oltre il confine limitato del lavoro su piattaforma.

In sostanza, in un futuro non troppo lontano, il lavoro su piattaforma, che negli ultimi anni ha attratto l'attenzione della dottrina giuslavoristica proprio per la peculiare assenza di tutele, sarebbe addirittura più tutelato del lavoro tradizionale.

E., ARMAROLI I., *A seat at the table: negotiating data processing in the workplace. A national case study and comparative insights*, in *Comparative Labor Law & Policy Journal*, 41, 2019, 173-195; PURIFICATO I., SENATORI I., *The Position of Collective Rights in the "Platform Work" Directive Proposal: Commission v Parliament*, in *Hungarian Labour Law e-Journal*, 1, 2023, 1-19.

131 Tesi avvalorata anche dalla dottrina, cfr. ad es. FAIOLI M., *Robot Labor Law. Linee di ricerca per una nuova branca del diritto del lavoro e in vista della sessione sull'intelligenza artificiale del G7 del 2024*, in *federalismi.it*, 8, 2024, 182-205.

INTELLIGENZA ARTIFICIALE E *REGULATORY SANDBOX*: PRIME OSSERVAZIONI CRITICHE

Giovanni Maria Riccio
Professore Ordinario di Diritto Comparato nell'Università degli Studi di Salerno

SOMMARIO: 1. *Regulatory sandbox*: cosa sono e quali sono i criteri di ammissione e selezione. - 2. Prime esperienze di *regulatory sandbox*. - 3. Protezione dei dati e *regulatory sandbox*. - 4. Il modello di responsabilità. - 5. Conclusioni.

1. *Regulatory Sandbox*: cosa sono e quali sono i criteri di ammissione e selezione.

Una delle soluzioni più interessanti introdotte dall'*Artificial Intelligence Act* è probabilmente rappresentata dall'introduzione, nel contesto tecnologico, delle *regulatory sandbox* o, per ricorrere alla dizione italiana, dagli spazi di sperimentazione normativa per l'intelligenza artificiale.

La definizione è contenuta nell'art. 3, par. 1, n. 55: "un quadro controllato istituito da un'autorità competente che offre ai fornitori o potenziali fornitori di sistemi di IA la possibilità di sviluppare, addestrare, convalidare e provare, se del caso in condizioni reali, un sistema di IA innovativo, conformemente a un piano dello spazio di sperimentazione per un periodo di tempo limitato sotto supervisione regolamentare".

Le *regulatory sandbox* rappresentano, quindi, un approccio innovativo per bilanciare innovazione e regolamentazione, precipuamente nel campo dell'intelligenza artificiale, favorendo lo sviluppo tecnico, ma garantendo, al contempo, che le nuove tecnologie aderiscano a standard normativi. Più specificatamente, questi strumenti permettono di testare nuove tecnologie prima della loro immissione sul mercato, al fine di monitorare sia la loro attitudine al rischio (ossia alla produzione di danni a terzi), sia la loro aderenza al rispetto dei principi fondamentali previsti dall'AI Act[132].

Non si tratta, però, di una novità assoluta, considerando che siamo al cospetto di un meccanismo introdotto legislativamente in settori diversi dall'intelligenza artificiale, seppur in altri ordinamenti giuridici; alcuni elementi, tuttavia, accomunano le diverse esperienze nazionali.

Difatti, stando ad uno studio commissionato dal governo tedesco, condotto su 27 sandbox regolamentari realizzate in vari settori, tra cui energia, trasporti e infrastrutture

[132] Su questo punto, per tutti, SIMONCINI A., *Il linguaggio dell'intelligenza artificiale e la tutela costituzionale dei diritti*, in *Rivista AIC,* 2023, n. 2, 1 ss.

logistiche[133], si tratta di soluzioni accomunate dalle seguenti caratteristiche: sono aree di sperimentazione create per un periodo limitato, focalizzate in un settore specifico, dove tecnologie innovative e modelli di business possono essere testati e messi a disposizione del pubblico; si basano sulla flessibilità regolamentare, non prevedendo sanzioni amministrative per il mancato rispetto delle normative vigenti; consentono ai regolatori (potere legislativo e autorità amministrative indipendenti) di acquisire conoscenze per sviluppare future norme e politiche pubbliche[134].

Sarebbe, tuttavia, riduttivo limitarsi a tali aspetti. I sistemi di intelligenza artificiale, soprattutto quelli ad alto rischio, nell'ipotesi che ci interessa, possono essere testati sotto supervisione regolatoria e, quindi, per mezzo di un dialogo costante tra l'industria e le autorità competenti di sorveglianza e di regolamentazione: una questione importante, considerando l'incognita di vanificare investimenti, spesso ingenti, e di elaborare un prodotto o un servizio che potrebbe non rispondere agli standard normativi. Ciò che si vuol segnalare, quindi, è che, nel caso dell'*Artificial Intelligence Act*, così come di altre emanande normative che consentono il ricorso a spazi di regolamentazione controllata[135], si sta passando da un approccio regolatorio focalizzato sul controllo successivo, da parte delle autorità amministrative, ad una cooperazione tra differenti *stakeholder* antecedente al lancio di un determinato prodotto o servizio o di una nuova tecnologia.

Quanto detto aprirebbe potenzialmente il campo a una discussione molto ampia che, per ovvie ragioni di sinteticità dell'esposizione, può solamente essere accennata in questa sede. Si allude all'ampia, spesso eccessiva, discrezionalità riconosciuta alle autorità amministrative indipendenti: basti riflettere sulle recenti vicende che hanno investito il settore della protezione dei dati personali, dove l'arbitrio nelle valutazioni del rispetto normativo rappresenta, non solo in Italia, un problema e un sensibile fattore di incertezza per le

133 BMWI - FEDERAL MINISTRY FOR ECONOMIC AFFAIRS AND ENERGY, *Making space for innovation: The handbook for regulatory sandboxes*, 2021, https://www.bmwk.de/Redaktion/EN/Publikationen/Digitale-Welt/handbook-regulatorysandboxes.pdf%3F__blob%3DpublicationFile%26v%3D2.

134 MORAES T., *Regulatory Sandboxes as Tools for Ethical and Responsible Innovation of Artificial Intelligence and their Synergies with Responsive Regulation*, in Belli L., Gaspar W.B. (a cura di), *The Quest for AI Sovereignty, Transparency and Accountability - Official Outcome of the UN IGF Data and Artificial Intelligence Governance Coalition*, 303 ss.

135 Si allude alla *Interoperability regulatory sandbox* di cui all'*Interoperability Act* (art. 2.14), dove si discorre di un ambiente controllato istituito da un ente dell'Unione o da un organismo del settore pubblico per lo sviluppo, la formazione, la sperimentazione e la convalida di soluzioni innovative di interoperabilità, se del caso in condizioni reali, a sostegno dell'interoperabilità transfrontaliera dei servizi pubblici digitali transeuropei per un periodo limitato periodo di tempo sotto controllo regolamentare e del *Cyber resilience regulatory sandbox* di cui al Cyber Resilience Act (art. 33.2), che prevede ambienti di prova controllati per prodotti innovativi con elementi digitali per facilitarne lo sviluppo, la progettazione, la convalida e i test allo scopo di conformarsi al presente regolamento per un periodo di tempo limitato prima dell'immissione sul mercato. Entrambi i testi normativi, nel momento in cui si scrive, sono in via di approvazione. Tuttavia, a differenza dell'AI Act, non prevedono che le *regulatory sandbox* siano obbligatorie per gli Stati membri, ma solo facoltative.

imprese[136]. Del resto, tale atteggiamento è favorito e incentivato dalla genericità delle formulazioni normative che, in numerosi settori, non da ultimo nell'AI Act, generano instabilità e complessità nella determinazione di investimenti[137].

In tale contesto, appare certamente apprezzabile – seppur con i limiti che saranno a breve evidenziati – il tentativo di sottrarre le imprese a tale incertezza, fissando *ex ante* standard e protocolli da seguire al fine di poter dimostrare il rispetto degli obblighi imposti. Come osservato correttamente, le *regulatory sandbox* possono essere uno strumento utile anche alle autorità pubbliche al fine di comprendere meglio le soluzioni adottate dai soggetti regolamentati, seguendo, passo dopo passo, lo sviluppo tecnologico di tali soluzioni e consentendo una comprensione *in vivo* e non *in vitro* dei servizi e dei prodotti rispetto ai quali si manifesta l'attività di controllo delle anzidette autorità[138].

Sul punto, è necessario peraltro precisare che molte delle questioni affrontate in questo breve scritto saranno precisate e (ci si augura) chiarite dalla Commissione europea negli Atti delegati di cui all'art. 97 AI Act, che assegna alla Commissione stessa un periodo, che dovrebbe essere di cinque anni dall'entrata in vigore del regolamento, per ulteriori interventi normativi, che dovrebbero incidere non solo sugli spazi di regolamentazione normativa, ma altresì su protocolli e linee-guida. Difatti, allo stato attuale, una delle maggiori preoccupazioni associate alle *regulatory sandbox* afferisce alla possibile discrasia tra le determinazioni che saranno assunte dalle autorità di sorveglianza nazionali e che potrebbero incidere sensibilmente sul processo di armonizzazione normativa. Peraltro, il potere discrezionale assegnato alle autorità nazionali potrebbe, almeno in linea teorica, determinare anche un fenomeno, sia consentita l'espressione non del tutto propria, di *forum shopping*: alcune imprese, soprattutto quelle con vocazione transazionale, potrebbero scegliere di operare in Paesi le cui autorità, al fine di agevolare l'economia nazionale, siano maggiormente permissive e aperte a soluzioni particolarmente ardite sul piano tecnologico e potenzialmente pericolose.

Di tale rischio, però, sembra essere consapevole il legislatore unionale che, non a caso, nell'art. 58, per evitare la frammentazione legislativa all'interno dell'Unione, ha previsto che la Commissione possa adottare atti di esecuzione, ai sensi dell'art. 291 TFUE, che possano

136 Sia consentito, per un quadro di sintesi, rinviare a RICCIO G.M., *Data protection and appropriate measures: too many uncertainties in the judicial applications?*, in *UNIO EULJ*, 2024, 17 ss., con i riferimenti ulteriori *ivi* citati.
137 Si pensi, ad esempio, ai provvedimenti che hanno riguardato – sempre in materia di *data protection* – i parametri della *privacy by design* e della *privacy by default* ovvero le questioni che hanno interessato gli strumenti probatori necessari a dimostrare l'aderenza (o, come si usa dire, la *compliance*) con gli obblighi legislativi. MANTELERO A., *The future of data protection: Gold standard vs. global standard*, in *Computer Law & Security Review,* 2020, 40, 1.
138 PARENTI R., R*egulatory sandboxes and innovation hubs for FinTech*, Study for the Committee on Economic and Monetary Affairs, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, 2020, 24.

precisare "le modalità dettagliate per l'istituzione, lo sviluppo, l'attuazione, il funzionamento e la supervisione degli spazi di sperimentazione normativa"[139].

Tali atti di esecuzione dovrebbero avere ad oggetto: a) i criteri di ammissibilità e selezione per la partecipazione allo spazio di sperimentazione normativa per l'IA (art. 58, par. 1, lett. a)); le procedure per la domanda, la partecipazione, il monitoraggio, l'uscita dallo spazio di sperimentazione normativa per l'IA e la sua cessazione, compresi il piano dello spazio di sperimentazione e la relazione di uscita (art. 58, par. 1, lett. b)); i termini e le condizioni applicabili ai partecipanti (art. 58, par. 1, lett. c)).

I criteri di selezione dovranno essere trasparenti ed equi: tuttavia, dalla lettura della disposizione sembra legittimo che gli Stati membri decidano di investire e quindi preferire determinati settori, anziché altri. Occorre tener presente, infatti, che si sta rapidamente passando da sistemi di intelligenza artificiale, per dir così, generalisti, a sistemi di intelligenza artificiale "verticali", pensati per determinati ambiti merceologici. Anzi, una simile soluzione, almeno a nostro avviso, sarebbe auspicabile: l'Italia, per rimanere in un ambito dominicale, potrebbe scegliere di preferire progetti legati al tessile o all'*automotive*, anziché pensare a investimenti a pioggia, che riguardino qualsiasi settore. Una scelta che dovrebbe consentire di applicare i medesimi standard anche alle altre imprese, operanti nella medesima area, che non partecipano alla sperimentazione normativa.

Resta, tuttavia, aperta la questione concorrenziale: infatti, i consumatori (o, in genere, il pubblico) potrebbero essere indotti a ritenere che prodotti e servizi, una volta testati e successivamente immessi sul mercato, abbiano un grado di affidabilità certificato da un'autorità pubblica e che, quindi, siano di qualità superiore rispetto agli altri[140].

Probabilmente, nel dettare i criteri, dovrà inoltre tenersi conto del grado di innovazione del progetto e del suo impatto sociale, pensando a clausole aperte che consentano l'accesso alle *regulatory sandbox* anche per progetti che, pur non rientrando nel novero dei settori preferiti, presentino un valore aggiunto o abbiano una possibilità concreta di realizzazione, determinando forti incentivi monetari e sociali sull'economia del singolo Stato membro.

2. Prime esperienze di *regulatory sandbox*.

I *regulatory sandbox*, come si diceva, non rappresentano una novità assoluta sul piano

[139] Sulla differenza tra atti di esecuzione e atti delegati, si rinvia a BAGNI F., *Commento all'art. 58*, in MANTELERO A., RESTA G., RICCIO G.M (a cura di), *Commentario all'AI Act*, Wolters-Kluwer, in corso di pubblicazione.

[140] Questo rischio è evidenziato da TRUBY J., BROWN R.D., IBRAHIM I.A., CAUDEVILLA PARELLADA O., *A Sandbox Approach to Regulating High-Risk Artificial Intelligence Applications*, in *European Journal of Risk Regulation*, 2022, 13, 270, 278. Sebbene gli Autori non la menzionino, occorre prendere in esame anche la possibilità che le *regulatory sandbox* possano ingenerare frizioni con la disciplina degli aiuti di Stato. Tale aspetto è affrontato anche da ALLEN H.J., *Regulatory Sandboxes*, 87 *George Washington Law Review*, (2019), 587 ss.

legislativo, essendo stati sperimentati (principalmente all'estero) da tempo e in molti settori, come il *fintech*, i trasporti, la sanità e l'energia.

L'elemento accomunante è l'alto grado di tecnicismo. La loro efficacia in questi ambiti fornisce un solido precedente per la loro applicazione nel settore dell'intelligenza artificiale. Alcuni Stati membri, come Austria, Danimarca, Ungheria, Lettonia, Lituania, Malta, Paesi Bassi e Spagna, hanno già adottato *regulatory sandbox*, in particolare per il *fintech*, evidenziando il loro potenziale successo nell'ambito dell'intelligenza artificiale. Al di fuori dell'Unione europea, sono stati istituiti in Paesi come Singapore, Australia, Emirati Arabi Uniti, Arabia Saudita, Hong Kong, Canada, India e Regno Unito. Gli Stati Uniti, pur non avendo un sandbox regolatore federale, hanno visto alcuni Stati come Arizona, Wyoming e Utah adottare tali strumenti regolamentari.

In particolare, nel Regno Unito, la *Financial Conduct Authority* (FCA) ha sperimentato per prima il *sandboxing* nel settore dell'innovazione finanziaria, a partire dal 2016. Ad oggi, la FCA ha supportato più di 700 imprese, accelerando la loro velocità media di ingresso sul mercato del 40% rispetto ai tempi di autorizzazione standard adottati prima del lancio della *sandbox*. Nello stesso anno si è mossa anche la *Monetary Authority* di Singapore, prevedendo agevolazioni sensibili per le imprese ammesse alla *sandbox*, che sono state esentate dal pagamento degli oneri amministrativi e finanziari imposti dai processi di conformità ordinari, potendo inoltre beneficiare di un campo di azione più ampio (non dovendosi rivolgere solo a un gruppo limitato di potenziali clienti, come gli altri soggetti autorizzati) e, di conseguenza, riuscendo ad affinare notevolmente le proprie soluzioni tecnologiche[141].

Gli esempi pregressi provano altresì che le società che partecipano ai *testing* hanno maggiori capacità di attrarre investimenti e, al tempo stesso, di proteggere gli elementi associati alla propria proprietà intellettuale, a partire dall'ambito brevettuale[142].

Tuttavia, alcuni studi dimostrano che tali vantaggi sono maggiori negli ordinamenti giuridici appartenenti alla famiglia di *common law*, rispetto a quelli appartenenti alla famiglia di *civil law*[143]. Non si tratta, tuttavia, di una novità per gli studi comparatistici, considerando la flessibilità del *common law* e l'attitudine dei Paesi, che appartengono alla relativa famiglia giuridica, a misurare l'innovazione seguendo parametri quali gli investimenti delle imprese in

[141] TRUBY J.*, FinTech and the city: sandbox 2.0 policy and regulatory reform proposals*, in *International Review of Law Compututer & Technology*., 2018, 34, 277.
[142] MONTERO SANTOS L., ROŽANEC J.M., *Fostering Research & Innovation in AI through Regulatory Sandboxes*, 16th International Technology Transfer Conference, Ljubljana, 11 ottobre 2023, https://ssrn.com/abstract=4604869.
[143] Sul concetto di famiglie giuridiche, si rinvia, per tutti a GAMBARO A., SACCO G., *Sistemi giuridici comparati*, Utet, 2018, *passim*.

ricerca e sviluppo e l'acquisizione di diritti di proprietà intellettuale[144].

Inoltre, le *regulatory sandbox* presentano forti analogie nel settore della protezione dei dati personali, in cui alcune autorità nazionali si sono mosse, proprio guidando esperienze sperimentali, con l'obiettivo di validare modelli di *privacy by design*[145]. La legislazione di settore, infatti, a partire dal Regolamento UE n. 2016/679, ha adottato un approccio basato sul rischio[146]: in estrema sintesi, l'idea di fondo muove dal presupposto che i soggetti che utilizzano (o, come si usa dire con terminologia tipica della *data protection*, trattano) i dati personali non sono tenuti ad adempiere obblighi specifici, ma ad assicurare un livello di protezione dei dati che sia ritenuto, dalle autorità di controllo, adeguato a prevenire e a mitigare i rischi connessi a tale trattamento.

Tuttavia, pare necessario puntualizzare che la prospettiva, nel caso in questione, è differente rispetto a quella adottata nel settore del *fintech* e, a partire dall'entrata in vigore dell'AI Act, per l'intelligenza artificiale. Difatti, nel caso delle esperienze anzidette relative alla protezione dei dati personali, non si è assistito ad un "allentamento" dei vincoli normativi, ma ad una cooperazione tra autorità di controllo e soggetti che, operando in ambiti legati all'innovazione, trattano dati personali, anche al fine di dettare delle *best practices* per gli altri operatori del settore. Le analogie, quindi, si arrestano all'impossibilità per le autorità pubbliche di comminare sanzioni nella fase di sperimentazione e nella maggiore consapevolezza acquisita da queste ultime, per mezzo di una conoscenza dettagliata dei prodotti e servizi tecnologici.

Né va dimenticato, da ultimo, che non mancano esperimenti di *data protection sandbox*: in Europa, il primo caso è quello norvegese, che, almeno al momento, sta offrendo degli interessanti spunti anche agli Paesi europei, rappresentando un modello imitabile con successo anche in altri ordinamenti giuridici[147].

3. Protezione dei dati e *regulatory sandbox*.

Molto complessa è la disciplina relativa al trattamento dei dati personali negli spazi di

[144] Tale profilo è ampiamente indagato da MARKELLOS R., ENNIS S., ENSTONE B., MANOS A., PAZAITIS D., PSYCHOYIOS D., *Worldwide Adoption of Regulatory Sandboxes: Drivers, Constraints and Policies*, Working Paper, Centre for Competition Policies, 2024, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4764911.

[145] Commissario per la Protezione dei Dati Personali di Singapore - PDPC (2017); l'Ufficio del Commissario per l'Informazione del Regno Unito – ICO (2019); il Datatilsynet della Norvegia (2021); la Superintendencia de Industria y Comercio della Colombia – SIC (2021); e la Commission Nationale de l'Informatique et des Libertés della Francia – CNIL (2022).

[146] Cfr. DE GREGORIO G., DUNN P., *The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age*, in *Common Market Law Revin*, 2022, 59, 473 ss.

[147] Cfr. https://www.datatilsynet.no/en/regulations-and-tools/sandbox-for-artificial-intelligence/ Su questa esperienza v. BAGNI F., *The Regulatory Sandbox and the Cybersecurity Challenge: from the Artificial Intelligence Act to the Cyber Resilience Act*, in *Rivista Italiana di Informatica e Diritto*, 2023, 206.

sperimentazione normativa. In un'immaginaria classifica delle norme che presentano le maggiori complessità – complessità non intrinseche, ma determinate dalla sciatteria della formulazione legislativa –, probabilmente l'art. 59 dell'AI Act si collocherebbe nelle prime posizioni.

Tale opinione, apparentemente eccessivamente critica, è il frutto di due riflessioni: la prima è che molti degli adempimenti previsti dalla norma sono già disciplinati in altre normative e riguardano, in generale, gli obblighi che persistono in capo ai titolari del trattamento in caso di utilizzazione dei dati; dall'altro canto, invece, si osserva che alcune delle soluzioni proposte – in particolare in materia di cancellazione – risultano, almeno a una prima lettura, impraticabili, rischiando di vanificare del tutto le attività realizzate nei *regulatory sandbox*.

Il settore della *data protection* sembra essere affetto, oramai da tempo, da un morbo incurabile, che è quello dell'autoreferenzialità dei soggetti che vi operano. In altri termini, si ha l'impressione che il diritto alla protezione dei dati, sancito nella Carta di Nizza, sia sottratto – almeno nella percezione degli operatori del settore – a logiche di bilanciamento tra valori contrapposti. Non si spiega altrimenti, una disposizione come la lett. g), laddove si impone la cancellazione dei dati utilizzati "una volta terminata la partecipazione allo spazio di sperimentazione o al raggiungimento del termine del periodo di conservazione dei dati personali".

Il problema, in questa fattispecie, è che, stando a quanto dichiarano i programmatori dei sistemi di IA, è impossibile cancellare i dati o, almeno, avere la certezza dell'avvenuta cancellazione, una volta terminato il periodo di "allenamento" delle macchine: l'obbligo imposto, quindi, potrebbe essere tecnicamente irrealizzabile. Anche a voler ritenere che quanto si sta dicendo non sia corretto, sempre da un punto di vista tecnologico, la cancellazione dei dati andrebbe comunque a influire negativamente sui processi di funzionamento dei sistemi, rischiando addirittura di vanificare i risultati raggiunti e testati all'interno della *regulatory sandbox*.

La successiva lett. h) impone, invece, la cancellazione dei log del trattamento dei dati personali al termine della partecipazione allo spazio di sperimentazione, "salvo diversa disposizione del diritto dell'Unione o nazionale". Anche in questo caso, siamo al cospetto di una scelta discutibile, atteso che i log sono strumenti necessari ai fini probatori, in caso di eventuali violazioni, che non rientrino nello spettro dell'esenzione dell'articolo in esame, o di danni procurati a terzi che, come a breve si vedrà, soggiacciono alle ordinarie regole di

responsabilità aquiliana[148].

Peraltro, a fare da eco a quanto detto, vi è anche la lett. e) della norma, dove si stabilisce che "i fornitori possono condividere ulteriormente i dati originariamente raccolti solo nel rispetto del diritto dell'Unione in materia di protezione dei dati; i dati personali creati nello spazio di sperimentazione non possono essere condivisi al di fuori dello spazio di sperimentazione". Una soluzione che mira alla tutela dei dati personali, ma che rischia di minare alle fondamenta il funzionamento dei sistemi testati all'interno della *sandbox*.

Peraltro, l'art. 59, lett. b), subordina la possibilità di trattare dati personali alla circostanza che non possa ricorrersi a dati anonimizzati, sintetici o di altri dati non personali, mantenendo i medesimi risultati.

In ogni caso, l'AI Act mira a integrare quanto previsto nel Regolamento UE n. 2016/679 con le disposizioni in materia di intelligenza artificiale. Premesso che l'IA non possa costituire una base giuridica per il trattamento dei dati, il Considerando n. 140, con una formulazione a dir poco complessa, che rimanda a numerose disposizioni preesistenti, non spiega (o almeno non è dato comprendere a chi scrive) quale sia la base giuridica adeguata[149].

L'art. 59 dell'AI Act non la identifica nel consenso, tuttavia ammette, a determinate condizioni, che siano utilizzati i dati personali raccolti per altre finalità. Tra le condizioni da soddisfare, è incluso, *in primis*, un elemento temporale e finalistico: difatti, i dati personali possono essere trattati unicamente ai fini dello sviluppo, dell'addestramento e delle prove di determinati sistemi di IA. La disposizione in commento include poi una limitazione settoriale, nel senso che i dati personali possono essere utilizzati nell'ambito di sistemi di intelligenza artificiale relativi alla salute o alla sicurezza pubblica; ambiente, biodiversità e contrasto all'inquinamento; sostenibilità energetica; mobilità, trasporto e infrastrutture critiche; miglioramento dell'efficienza e della qualità della pubblica amministrazione e dei servizi pubblici.

Peraltro, l'elencazione risulta talmente generica da rappresentare una difficile delimitazione: si pensi, ad esempio, a quante società rientrano nel novero delle infrastrutture critiche e quante attività differenti svolgano. Un chiarimento è però dato dalla lett. a) del par. 1, dove si afferma che i sistemi di intelligenza artificiale devono essere "sviluppati per salvaguardare un interesse pubblico": pertanto, il perimetro relativo alle attività deve

[148] Su questo aspetto, risultano interessanti alcune pronunce di tribunali nazionali (es. in Polonia e Ungheria) relativi all'onere della prova nell'ambito dei procedimenti dinanzi alle autorità di controllo per la protezione dei dati personali, su cui *amplius* sia consentito rinviare a RICCIO G.M., *Data protection and appropriate measures*, cit., 21.

[149] Sul punto di rinvia a SORRENTINO G., *Commento all'art. 59*, in MANTELERO A., RESTA G., RICCIO G.M., *Commentario all'AI Act*, Wolters-Kluwer, in corso di pubblicazione.

convivere necessariamente con la finalità che non può essere di matrice privatistica, ma deve coinvolgere, seppur indirettamente, una finalità superiore.

Permane, ciò nonostante, un ampio margine di incertezza: ad esempio, un dispositivo medico che utilizza l'intelligenza artificiale, sviluppato da un privato, senza un investimento pubblico, rientra o meno in tale perimetro normativo? A nostro avviso, la risposta non può che essere affermativa, riflettendo sull'obiettivo delle *regulatory sandbox* che, almeno nei sistemi giuridici nazionali, hanno avuto quale obiettivo principale quello di favorire il rapporto tra le imprese (e non gli enti pubblici) e le autorità pubbliche di sorveglianza o di controllo.

L'art. 59 dell'AI Act contempla poi alcuni obblighi che erano già previsti nella normativa in materia di protezione dei dati personali, come l'obbligo di condurre una valutazione di impatto e l'adozione di misure di sicurezza, tecniche e organizzative. Tra queste dovrebbe rientrare, sebbene inclusa poi in una previsione *ad hoc* (lett. d)), anche il divieto di accesso a tali dati da parte di persone non autorizzate e il trattamento dei dati in "ambiente di trattamento dei dati funzionalmente separato, isolato e protetto sotto il controllo del potenziale fornitore" (ad esempio, segregando i diversi database che trattano i dati personali).

4. Il modello di responsabilità.

Un aspetto di indubbio interesse afferisce alle responsabilità associate alla fase di sperimentazione normativa. L'art. 57, par. 12, prevede che i fornitori siano responsabili, ai sensi della normativa interna e di quella unionale, in caso di danni a terzi "a seguito della sperimentazione che ha luogo nello spazio di sperimentazione".

La norma, quindi, prevede che questi soggetti siano tenuti a risarcire eventuali lesioni secondo le ordinarie regole della responsabilità aquiliana: tuttavia, chi scrive ritiene che sia preferibile ampliare la portata applicativa della disposizione in commento, ricomprendendovi non solo i danni successivi alla sperimentazione – come l'interpretazione letterale vorrebbe suggerire –, ma, altresì, i danni occorsi durante tale fase.

È risaputo che, nei singoli ordinamenti giuridici membri dell'Unione europea, la definizione di responsabilità e quella di danno sfuggano ad una definizione precisa[150].

[150] La nozione di danno – anche a livello comparatistico – sfugge ad una precisa definizione. Uno sforzo nel quale si è cimentato il solo Codice civile austriaco, peraltro con una formula che si presta a molteplici interpretazioni; cfr. §1293 Allgemeines bürgerliches Gesetzbuch, ABGB. Allo stesso modo, risulta difficile identificare univocamente, all'interno del diritto unionale, un'esplicitazione del concetto di danno e, talvolta, nelle sue pronunce, la Corte di Giustizia lo ha inteso quale corrispettivo del concetto di lesione. Finanche la direttiva in materia di responsabilità del produttore, dove pure il danno ha un ruolo fondamentale, non aiuta in tal senso. Ciò determina che, tendenzialmente, la determinazione dei confini del danno risarcibile non potrà che continuare a essere rimesso all'apprezzamento delle corti nazionali. Sul punto, v. VAQUER A., *Damage*, in KOZIOL H., SCHULZE R. (a cura di), *Tort Law of the European Community. Tort and Insurance Law*, vol. 23. Springer, Vienna, 2008, 30.

Peraltro, l'art. 57, par. 12, dovrà necessariamente essere integrato con la proposta di direttiva in materia di intelligenza artificiale, il cui obiettivo è quello di armonizzare le normative nazionali, alla luce dell'osservazione che dette normative, "in particolare per colpa, non sono adatte a gestire le azioni di responsabilità per danni causati da prodotti e servizi basati sull'IA".

L'obiettivo della proposta di direttiva anzidetta, peraltro, non è quello di armonizzare i sistemi di responsabilità extracontrattuale, ma unicamente quello di fissare alcuni principi in materia di onere probatorio. La nuova normativa, infatti, dovrebbe trovare applicazione a tutti i sistemi di intelligenza artificiale, disponendo obblighi di divulgazione di elementi di prova relativi a sistemi di intelligenza artificiale ad alto rischio, per evitare il rischio di *black-box* ossia al fine di scongiurare che la dimostrazione della condotta del potenziale danneggiante costituisca una *probatio diabolica* in capo al danneggiato. I sistemi di intelligenza artificiale, prima della loro immissione sul mercato, vedono, da un lato, l'interazione di diversi operatori, il che incide significativamente in termini di dimostrazione del nesso eziologico tra condotta del danneggiante, evento e danno, e, dall'altro, che l'opacità, il comportamento autonomo e la complessità, possano "rendere eccessivamente difficile, se non impossibile, per il danneggiato soddisfare l'onere della prova"[151].

Nello specifico, all'art. 3 della Proposta, si prevede un meccanismo che, per mezzo del ricorso all'autorità giudiziaria, possa ristabilire le asimmetrie informative sussistenti tra utenti e operatori imponendo a un fornitore di divulgare "gli elementi di prova pertinenti di cui dispone in relazione a un determinato sistema di IA ad alto rischio che si sospetta abbia cagionato il danno". Tale ordine giudiziario può essere concesso in presenza di un rifiuto da parte degli operatori dei sistemi di rivelare tali informazioni, laddove sussistano "atti e prove sufficienti a sostenere la plausibilità della domanda di risarcimento del danno" (una sorta, quindi, di fumus boni juris) e della circostanza che l'attore abbia "previamente compiuto ogni sforzo proporzionato per ottenere tali elementi di prova dal convenuto" (parr. 1 e 2, art. 3).

L'esenzione di responsabilità fissata dall'art. 57, par. 12 AI Act interessa, invece, esclusivamente le eventuali sanzioni amministrative, che non potranno essere comminate dall'autorità di controllo, a condizione che i fornitori "rispettino il piano specifico e i termini e le condizioni di partecipazione e seguano in buona fede gli orientamenti forniti dall'autorità nazionale competente, quest'ultima non infligge alcuna sanzione amministrativa in caso di

[151] Considerando n. 3 della Proposta, dove si afferma altresì che "In particolare può essere eccessivamente difficile dimostrare che un determinato input, di cui è responsabile la persona potenzialmente tenuta a rispondere del danno, ha provocato un determinato output del sistema di IA, che a sua volta ha causato il danno in questione".

violazione" degli obblighi fissati dal Regolamento. Del resto, considerando che le *regulatory sandbox* si fondano sulla diretta comunicazione e interazione tra le stesse autorità di controllo e i fornitori, risulterebbe comunque improbabile immaginare una sanzione da parte di tali autorità, salvo i casi di dolo da parte del fornitore nel corso della sperimentazione, accertato successivamente alla commissione della relativa condotta.

5. Conclusioni.

Quando si riflette sulla portata delle *regulatory sandbox*, un punto di partenza necessario è rappresentato dagli studi seminali sviluppatisi agli albori degli anni Ottanta, principalmente da parte di David Collingridge (da cui l'omonimo paradosso di cui si dirà a breve)[152]. L'idea di fondo è la seguente: il legislatore cerca di controllare la tecnologia al fine di contenere l'emersione di danni sociali e, quindi, partendo dall'idea che il diritto possa limitare eventuali situazioni critiche determinate dallo sviluppo tecnologico. Tuttavia, si scontra con una situazione ambivalente, che parte dalla mancanza di informazioni precise, su cui selezionare opzioni normative, finché la tecnologia non è ampiamente sviluppata e utilizzata. In altre parole, è arduo regolamentare qualcosa che – come le tecnologie dell'intelligenza artificiale – è in una fase di potenziamento e i cui effetti sono ancora impossibili da predire, se non per mezzo di approssimazioni che spesso potrebbero indurre esclusivamente a limitare lo sviluppo di tali soluzioni.

Dall'altro lato, una volta che una tecnologia si è diffusa, risulta altrettanto complesso limitarne il suo impatto sociale. Chi sarebbe disposto – seppur dopo un tempo molto limitato di utilizzazione – a rinunciare oggi all'ausilio dell'intelligenza artificiale generativa? Storicamente, infatti, tutte le volte che l'uomo ha inventato un oggetto, a partire dalla ruota, non è mai tornato indietro[153].

Con l'avvento di internet, a partire dai primi anni Novanta, è stato così; la diffusione dei social media e della c.d. *new economy* ha determinato un effetto analogo nel decennio successivo. Oggi ci scontriamo con i dilemmi dell'intelligenza artificiale e ci troviamo a ripercorrere sentieri normativi i cui solchi rimandano, sinistramente, a quanto avvenuto nei decenni scorsi in Europa e dall'altra sponda dell'Atlantico.

Si pensi, ad esempio, all'avvento dei social network e, in generale, di internet: nell'arco temporale a cavallo tra i due millenni, alcuni ordinamenti – principalmente gli Stati Uniti, mossi da un approccio neoliberista – hanno adottato politiche di *laissez-faire*, evitando di

[152] COLLINGRIDGE, D.*, The Social Control of Technology,* St. Martin's Press, New York, 1980.
[153] INGOLD T., *Making: Anthropology, archaeology, art and architecture*, Routledge, London, 2013.

intervenire in maniera sensibile sul mercato, ma, al contempo, perdendo qualsiasi controllo dei mezzi, anzi, finendo per esserne risucchiati.

L'avvento dei sistemi di intelligenza artificiale appare, quindi, come un *deja-vu* per chi ha assistito allo sviluppo di internet. Alla fine del millennio scorso, gli Stati Uniti promulgarono alcune normative molto permissive per i fornitori di servizi (*internet service provider* o ISP), come il *Communications Decency Act* sulla diffamazione e il *Digital Millennium Copyright Act* del 1998 in materia di diritto d'autore. Quest'ultima legge fu quasi pedissequamente imitata in Europa dalla Direttiva sul commercio elettronico (2000/31/CE), che, negli articoli 12-15, stabiliva il principio di non responsabilità per gli ISP in caso di neutralità, ossia quando si limitavano a ruoli meramente tecnici.

Queste disposizioni favorirono l'ascesa dei grandi fornitori americani e, qualche anno dopo, dei motori di ricerca e dei social network. Del resto, non è un caso che tutti i monopolisti o le aziende con una posizione dominante in questi mercati siano società statunitensi, poiché lo sviluppo tecnologico, obiettivamente superiore rispetto a quello delle imprese europee, è stato accompagnato da una legislazione favorevole che ha permesso la crescita esponenziale di questi operatori.

Nell'ultimo decennio, l'Europa ha optato per un approccio antitetico, non allineandosi alle scelte statunitensi, ma creando un modello giuridico autonomo. Se si analizza l'AI Act, solo le aziende non europee sono, al momento, obbligate a monitorare lo sviluppo dei loro modelli di intelligenza artificiale e il loro impatto sui diritti fondamentali, il che rischia addirittura di tradursi in una forma di politica protezionistica sostenuta dalle istituzioni europee, mascherata come protezione dei diritti fondamentali.

Il rinomato effetto Bruxelles[154] ha eretto un muro nella protezione dei valori sanciti dalla Carta di Nizza, creando un ambiente digitale più sicuro per tutti i cittadini dell'UE che sono utenti dei servizi digitali. Tuttavia, in questo settore, sembra esserci un elemento controverso, nel senso che si ha la sensazione generale che l'Europa, anziché promuovere l'innovazione e la competitività, stia affrontando il suo ritardo rispetto agli Stati Uniti e ad altri paesi asiatici (soprattutto Cina e Corea) impedendo l'invasione di queste tecnologie prodotte (e controllate) da paesi terzi.

È difficile (e onestamente ingiusto) criticare gli obiettivi della Commissione Europea alla base dell'AI Act. Nessuno potrebbe essere in disaccordo con obblighi rigorosi sui sistemi di intelligenza artificiale ad alto rischio, così come evitare le asimmetrie informative degli utenti

[154] BRADFORD A., *The Brussels Effect: How the European Union Rules the World*, Oxford University Press, Oxford, 2020.

quando interagiscono con un bot e introdurre misure legali per contrastare la disinformazione. Tuttavia, il fattore tempo deve essere considerato: l'AI Act non diventerà pienamente operativo per almeno due anni, che, nel settore tecnologico, potrebbe corrispondere ad un'era geologica.

Non esistono ancora protocolli condivisi e molte incertezze circondano le pratiche da adottare per bilanciare i diritti fondamentali dei cittadini con i diritti dei fornitori. Non è inoltre chiaro come la Commissione o l'Ufficio europeo per l'IA interverranno per fornire regole chiare, che sono assolutamente necessarie per garantire un ambiente sicuro in questo settore. Però una cosa è certa: per essere competitivi con le imprese extraeuropee e per poter calibrare opportunamente gli investimenti, sia pubblici sia privati, occorrono regole certe che, al momento, non si intravedono ancora.

AI ACT E DATIFICAZIONE DEL LAVORO

Ilaria Del Giglio
Avvocato, Dottoressa di ricerca in Lavoro Sviluppo e Innovazione, Università degli Studi di Modena e Reggio Emilia, Fondazione Marco Biagi

SOMMARIO: 1. Dalla digitalizzazione alla datificazione del lavoro e AI Act. - 2. Sistemi di IA ad "alto rischio" e tutele dei lavoratori. - 3. Applicativi impiegati in ambienti di lavoro che utilizzano sistemi di IA. - 3.1. HRIS *(Human Resources Information System).* - 3.2. *Digital Workplace.* - 3.3. CRM (*Customer Relationship Management*). - 4. Interventi dell'AI Act e tutele dei lavoratori. In particolare: la trasparenza dei sistemi di IA.

1. Dalla digitalizzazione alla datificazione del lavoro e AI Act.

Le norme introdotte dal Regolamento Europeo sull'Intelligenza Artificiale (AI Act) si inseriscono in un contesto lavorativo profondamente innovato e divenuto, grazie alla tecnologia, sempre più connesso e digitale. La digitalizzazione ha, infatti, reso accessibili nuove potenzialità che innervano profondamente il mondo del lavoro: dal luogo in cui viene eseguita la prestazione, al modo in cui questa viene adempiuta, dalle possibilità di osservare i lavoratori, alle capacità di analisi. Potenzialità ulteriormente implementate dai sistemi di Intelligenza Artificiale.

Lo sviluppo introdotto dall'Industria 4.0[155] ha portato, quindi, a una radicale trasformazione delle imprese che, grazie alla tecnologia dell'Informazione e Comunicazione (ICT), ha modificato le modalità di esecuzione del lavoro e la gestione del personale.

La prima novità introdotta dalle tecnologie ICT è il venir meno dei parametri che hanno sempre caratterizzato e misurato la prestazione lavorativa: il luogo e il tempo. Grazie alla

[155] TULLINI P., *Il controllo a distanza attraverso gli strumenti per rendere la prestazione lavorativa. Tecnologie di controllo e tecnologie di lavoro: una distinzione possibile*, in TULLINI P., (a cura di) *Controlli a distanza e tutela dei dati personali*, Giappichelli Editore, Torino, 2017, 118 nota 67; DESSI O., *Il controllo a distanza sui lavoratori. Il nuovo art. 4 Stat. lav.*, Edizioni Scientifiche Italiane, Napoli, 2017, 177-181; SEGHEZZI F., *La nuova grande trasformazione. Lavoro e persona nella quarta rivoluzione industriale*, ADAPT University Press, 2017, 150, in cui l'autore sottolinea l'impatto della nuova tecnologia sui sistemi produttivi e organizzativi; MARTINI D., *Industria 4.0: una prima riflessione critica,* in L'industria, n. 3, 2016, 385; DEL PUNTA R., *Un diritto per il lavoro 4*.0, in CIPRIANI A., GRAMOLATI A., MARI G. (a cura di), *Il lavoro 4.0. La IV rivoluzione industriale e le trasformazioni delle attività lavorative*, FUP, Firenze, 2017, 225 ss.; LOMBARDI M., MACCHI M., *Il lavoro tra intelligenza umana e intelligenza artificiale*, in CIPRIANI A., GRAMOLATI A., MARI G. (a cura di), *Il lavoro 4.0. La IV rivoluzione industriale e le trasformazioni delle attività lavorative*, FUP, Firenze, 2017, 225 ss.; TIRABOSCHI M., SEGHEZZI F., *Il Piano nazionale Industria 4.0: una lettura lavoristica*, in *LLI,* vol. 2, n. 2, 2016, 13 ss.; INGRAO A., *Il Controllo distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata*, Cacucci Editore, Bari, 2018, 68 -74; DAGNINO E., *Dalla fisica all'algoritmo: una prospettiva di analisi giuslavoristica,* ADAPT University Press, 2019, 39-44; SANTUCCI R., *La quarta rivoluzione industriale e il controllo a distanza dei lavoratori*, in *Il Lavoro nella giurisprudenza*, n. 1, 2021, 19 ss.; CIRPIANI A., GRAMOLATI A., MARI A. (a cura di), *La Quarta Rivoluzione industriale e le trasformazioni delle attività lavorative*, Firenze University Press, 2018, disponibile *online.*

digitalizzazione, in un numero crescente di casi l'attività lavorativa può essere eseguita "in ogni luogo, in ogni tempo e con ogni dispositivo"[156].

In secondo luogo, le tecnologie introdotte dall'Industria 4.0 amplificano le potenzialità di acquisire, elaborare e condividere dati. Le tecnologie abilitanti poste a servizio dei lavoratori rendono possibile l'esecuzione di prestazioni "native digitali" in ambienti virtuali, al contempo datificandole. La digitalizzazione sviluppa, infatti, il contestuale fenomeno della datificazione[157] dei rapporti di lavoro, convertendo in dati le attività compiute in ambienti virtuali. Il lavoro può, quindi, essere osservato mediante nuovi *output* che codificano l'azione, ovvero i dati provenienti dai "*virtual office*"[158].

Nel processo di innovazione del lavoro vi è, dunque, una costante: l'utilizzo di dati e il necessario intervento di una fase intermedia, spesso interamente demandata a sistemi di IA, per poter comprendere il significato delle informazioni. Tra acquisizione e utilizzo dei dati vi è, quindi, un momento di elaborazione capace di "tradurne" il significato e idoneo a disvelare nuove informazioni prima non comprensibili.

Tale trasformazione del lavoro conduce ad alcune conseguenze.

Prima fra tutte, la digitalizzazione e la datificazione del lavoro permettono (potenzialmente) di osservare e comprendere ogni aspetto dei lavoratori digitali, non solo connesso all'ambito professionale. Tali aspetti non risultano, però, sempre "immediatamente comprensibili", ma lo diventano solo all'esito di un necessario processo interpretativo. Datificare l'attività lavorativa non restituisce, infatti, dati immediatamente "autoevidenti"[159]. A differenza dell'osservazione a distanza di una prestazione "analogica" (compiuta

---

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

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

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

159 Nel presente articolo la terminologia dati "autoevidenti" costituisce una classificazione non normativa qui impiegata per identificare tutti quei dati che restituiscono un'informazione in maniera immediata, senza la necessità di un processo di analisi o di correlazione preliminare.
Nel contesto lavorativo si possono qualificare come dati "autoevidenti", per esempio, le immagini che possono essere acquisite mediante una videocamera di sorveglianza o con uno screenshot dello schermo di un pc.
Costituiscono, quindi, sicuramente dati "autoevidenti" tutti quelli di natura personale sia in senso oggettivo (come gli elementi caratteristici dell'identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale di un soggetto) sia soggettivo (come opinioni o valutazioni).

fisicamente sul luogo di lavoro) che restituirà un'immagine, un suono o, comunque, un dato immediatamente interpretabile, l'acquisizione delle "tracce digitali" lasciate dai lavoratori in contesti virtuali non risulta sempre *ictu oculi* significativa. La fase di elaborazione e interpretazione dei dati mediante il supporto di *software* o sistemi di IA diviene, pertanto, un passaggio essenziale per giungere alla comprensione dei medesimi che risultano, altrimenti, "non autoevidenti"[160].

2. Sistemi di IA ad "alto rischio" e tutele dei lavoratori.

L'AI Act, pur essendo il primo Regolamento volto a normare i sistemi di Intelligenza Artificiale, non è la prima legge che regola l'impiego di strumenti in ambito lavorativo.

AI Act si inserisce, infatti, in un sistema volto a normare l'utilizzo di strumenti di lavoro, soprattutto ove da questi possa derivare un controllo.

In merito, la norma cardine è l'art. 4 dello Statuto dei Lavoratori che traccia un limite tra strumenti di lavoro e strumenti di controllo la cui tutela giuslavoristica viene integrata, mediante il rinvio compiuto al comma 3, dalla normativa *privacy*[161] che disciplina l'utilizzo dei dati acquisiti.

La norma statutaria, dettata per prestazioni "analogiche" che acquisiscono la natura digitale solo in un secondo momento, per mezzo dello strumento impiegato[162] manifesta, però, alcuni *vulnus* di tutela quando la prestazione si configura come "nativa digitale"[163] .

È possibile osservare tale "*gap*" di tutela soprattutto in riferimento ai dati "non autoevidenti".

L'art. 4 dello Statuto dei Lavoratori compie, infatti, una valutazione *ex ante* (ossia prima che i dati vengano utilizzati) in merito alla natura dei dati acquisiti, al fine di definire se da questi possa derivare un controllo del lavoratore e se tale controllo possa essere ricondotto a una delle esigenze tipizzate dalla norma164.

---

160 Il termine dato "non autoevidente" costituisce una classificazione non normativa e qui impiegata per individuare quei dati non immediatamente comprensibili e per la cui interpretazione è necessaria una fase preliminare di elaborazione/correlazione così che possano restituire un'informazione riferibile a una persona identificata/identificabile.
La categoria dei dati "non autoevidenti" ha quale caratterista comune la non immediata intelligibilità, ossia l'assenza di significato, circostanza che può inibire sia l'identificabilità (di conseguenza anche la corrispondenza univoca) con un soggetto, sia la possibilità di fornire un'informazione allo stesso concernente.
Possono essere considerati, per esempio, dati "non autoevidenti" gli *exaust data* ossia quei dati di "scarto" che derivano da operazioni informatiche, privi di significato ove raccolti autonomamente perché non rivelatori di alcuna informazione attinente ad una persona fisica o perché non possono ritenersi immediatamente riguardanti la medesima o perché inidonei a identificarla.
161 Regolamento UE 679/2016 (GDPR), D.Lgs. 196/2003 e s.m.i. (Codice privacy).
162 Come può avvenire con un'immagine ripresa da una videocamera.
163 Ossia quando questa sorge e si compie interamente in un ambiente virtuale.
164 Cfr. art. 4 comma 1 St. Lav.: esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale.

Ove, però, i dati non siano immediatamente comprensibili, ovvero "non autoevidenti", per ottenere un'informazione significante è necessario svolgere una preliminare elaborazione interpretativa.

La valutazione compiuta a priori su un dato "non autoevidente", apparentemente neutro, potrebbe così risultare errata, non essendo in grado di disvelare il reale significato del dato prima dell'elaborazione.

La riflessione appena compiuta fa comprendere quanto profondamente la digitalizzazione inerisca le tutele dei lavoratori.

AI Act si affianca così al corpus normativo redatto per prestazioni analogiche, apportando un sistema di tutele finalizzate a far fronte alle nuove esigenze poste da una tecnologia sempre più abilitata a compiere "sofisticate operazioni di rielaborazione e confronto per aggregazione dei dati"165.

L'AI Act, sebbene nasca quale normativa di dettaglio volta a regolamentare lo sviluppo, la commercializzazione e l'uso dei sistemi di intelligenza artificiale (IA), nella sua versione definitiva non tralascia di affrontare aspetti specifici che ineriscono il mondo del lavoro datificato e le precauzioni che devono essere adottate sia dagli sviluppatori di sistemi di IA che dai *deployer* [166], ossia dai datori di lavoro.

Il tema della protezione dei lavoratori viene affrontato a partire Considerando 9 ove si afferma che le regole di armonizzazione stabilite dal nuovo Regolamento sull'AI dovrebbero trovare applicazione in tutti i settori e non dovrebbero pregiudicare la normativa vigente dell'Unione, in particolare in materia di occupazione e protezione dei lavoratori[167]. Le potenzialità degli strumenti impiegati dai lavatori dotati di sistemi di IA, possono, infatti, "contribuire a migliorare le condizioni di lavoro" ove accompagnate da un'"ampia attuazione delle misure di alfabetizzazione in materia di IA" e "di adeguate azioni di followup" (Considerando 20).

Le potenzialità offerte dai sistemi di AI di acquisire informazioni e di osservare i lavoratori in modo pervasivo impongono, però, la necessità di introdurre precisi limiti e divieti. Ciò al fine di tutelare i diritti dei lavoratori dall'impatto negativo che può derivare dal sistema di IA

165 ZANETTI P., *Impresa, lavoro e innovazione tecnologica*, Giuffrè Editore, Milano, 1985, 68-70.
166 AI Act all'articolo 3 punto 4 definisce "deployer" come la "persona fisica o giuridica, autorità pubblica, agenzia o altro organismo che utilizza un sistema di IA sotto la propria autorità, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale".
167 Il medesimo Considerando prosegue dichiarando che "nel contesto dell'occupazione e della protezione dei lavoratori, il presente regolamento non dovrebbe pertanto incidere sulla normativa dell'Unione in materia di politica sociale né sulla normativa nazionale in materia di lavoro, in conformità del diritto dell'Unione, per quanto riguarda le condizioni di impiego e le condizioni di lavoro, comprese la salute e la sicurezza sul luogo di lavoro, e il rapporto tra datori di lavoro e lavoratori".

(Considerando 48). Il Considerando 44 prevede, dunque, che dato "lo squilibrio di potere nel contesto del lavoro o dell'istruzione, combinato con la natura invasiva di tali sistemi" da cui può derivare "un trattamento pregiudizievole o sfavorevole" risulta "pertanto opportuno vietare l'immissione sul mercato, la messa in servizio o l'uso di sistemi di IA destinati a essere utilizzati per rilevare lo stato emotivo delle persone in situazioni relative al luogo di lavoro (…)". Alla luce di ciò, i sistemi impiegati "nel settore dell'occupazione, nella gestione dei lavoratori (…) 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" (Considerando 57).

Il Regolamento prosegue sottolineando l'importanza di una comprensione e di una reale partecipazione dei lavoratori, auspicando che questi vengano coinvolti "in modo significativo". Coinvolgimento che passa attraverso un dovere di trasparenza e informazione rimesso ai *deployer* (utilizzatori), ossia ai datori di lavoro. Il Considerando 92 lascia, dunque, impregiudicati "gli obblighi dei datori di lavoro di informare o di informare e consultare i lavoratori o i loro rappresentanti (…)" ritenendo "necessario garantire che i lavoratori e i loro rappresentanti siano informati in merito alla diffusione programmata dei sistemi di IA ad alto rischio sul luogo di lavoro".

L'AI Act entra, poi, nel merito dei sistemi di IA impiegati in ambito lavorativo prevedendo all'articolo 2 punto 11 che l'Unione o gli Stati membri mantengano o introducano disposizioni "più favorevoli ai lavoratori in termini di tutela dei loro diritti in relazione all'uso di sistemi di IA da parte dei datori di lavoro, o incoraggino o consentano l'applicazione di contrati collettivi più favorevoli ai lavoratori". Il Regolamento, pertanto, arretra dinanzi alle peculiari tutele vigenti in ambito giuslavoristivco nei singoli Paesi, permettendo deroghe in favore dei lavoratori.

AI Act prosegue elencando all'articolo 5 le pratiche di Intelligenza Artificiale vietate e inserendo tra queste quelle destinante a "inferire le emozioni di una persona fisica nell'ambito del luogo di lavoro". La norma pone, dunque, un divieto all'immissione e messa in servizio di sistemi di IA destinati a comprendere e analizzare quelli che possono essere, per esempio, il grado di soddisfazione o meno di un lavoratore nei confronti della propria attività.

Il Regolamento prosegue, poi, all'articolo 6 classificando i sistemi di IA ad alto rischio, identificando come tali – in forza del rinvio compiuto all'Allegato III[168] –, i sistemi di IA utilizzati nel contesto lavorativo, come quelli per il reclutamento, la gestione delle prestazioni e la valutazione dei dipendenti. Questi sistemi, proprio per l'alto livello di rischio connesso al loro impiego e al loro potenziale impatto su diritti fondamentali dei soggetti coinvolti, devono essere soggetti a regolamentazioni[169] più stringenti, soprattutto in riferimento ai livelli di trasparenza (articolo 13)[170] e sulla sorveglianza umana (articolo 14).[171]

Le tutele contenute negli articoli da ultimi richiamati prevedono, dunque, di porre i lavoratori nella condizione non solo di sapere che il datore sta impiegando sistemi di IA, ma anche di conoscerne il funzionamento e la logica sottesa alle decisioni da questo prese. Ciò al fine di poter intervenire a tutele della propria posizione e di poter chiedere una revisione delle decisioni assunte tramite un intervento umano. Le previsioni cercano, così, di escludere un totale meccanicismo secondo un approccio antropocentrico.

In ragione della natura "ad alto rischio" il *deployer*/datore di lavoro risulta obbligato a compiere precise misure poste a garantire la tutela dei lavoratori coinvolti nei trattamenti con sistemi di IA. I datori di lavoro devono, infatti, adottare "idonee misure tecniche e organizzative per garantire di utilizzare tali sistemi conformemente alle istruzioni per l'uso che accompagnano i sistemi" nonché affidano "la sorveglianza umana a persone fisiche che dispongono della competenza, della formazione e dell'autorità necessarie nonché del sostegno necessario" (articolo 26 parag. 1 e 2). Al datore di lavoro spetta, in particolare, il compito di informare "i rappresentanti dei lavoratori e i lavoratori interessati che saranno

[168] Allegato III del Regolamento sull'Intelligenza Artificiale elenca, infatti, i sistemi di Intelligenza Artificiale considerati ad alto rischio in vari settori, tra cui quello del lavoro. Si legge, infatti, al punto 4: "Occupazione, gestione dei lavoratori e accesso al lavoro autonomo: a) i sistemi di IA destinati a essere utilizzati per l'assunzione o la selezione di persone fisiche, in particolare per 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".

[169] Per i sistemi di IA ad "alto rischio" è previsto che venga implementato un sistema di gestione che includa l'identificazione, la valutazione e la mitigazione dei rischi associati all'uso dell'IA (art. 9); che i dati utilizzati per addestrare i sistemi di IA siano di alta qualità, rappresentativi, pertinenti e non discriminatori (art. 10); che venga fornita idonea documentazione tecnica da parte dei fornitori (art. 11); che vengano istituiti registri delle attività di trattamento dei dati compiute dai sistemi di IA ad alto rischio (art. 12); che i sistemi di IA siano robusti, sicuri e accurati. Questo significa che devono funzionare in modo affidabile anche in condizioni avverse e non ledere i soggetti coinvolti (art. 15). Il rispetto di tali requisiti è rimesso alle autorità di vigilanza nazionali e l'Unione Europea devono monitorare la conformità dei sistemi con l'AI Act (art. 54).

[170] I *deployer* devono fornire informazioni chiare e trasparenti su come funzionano i sistemi di IA e su come vengono prese le decisioni, anche in riferimento ai criteri valutativi impiegati.

[171] I sistemi di IA ad alto rischio devono essere soggetti a una sorveglianza umana adeguata a garantire che possano essere arrestati o corretti ove possano ledere i diritti dei soggetti coinvolti o compiere *bias* di valutazione con esiti anche discriminatori.

soggetti all'uso del sistema di IA ad alto rischio" prima di mettere in servizio o utilizzare un sistema di IA ad alto rischio sul luogo di lavoro (articolo 26 parag. 7).

Informazioni che devono 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.

3. Applicativi impiegati in ambienti di lavoro che utilizzano sistemi di IA.

Data la natura di "alto rischio" riconosciuta dall'AI Act ai sistemi di IA applicati in contesti lavorativi, il presente articolo intende procedere con un'analisi sulla prassi dei sistemi di IA impiegati i contesti lavorativi al fine di comprendere se la nuova regolamentazione riesca a colmare le possibili vulnerabilità che derivano dalla datificazione del lavoro. Per indagare tale aspetto, risulta necessario comprendere preliminarmente quali siano gli strumenti impiegati in un contesto digitale.

A tal fine, sono stati esaminati i principali sistemi informativi per la gestione del personale e per l'esecuzione delle prestazioni native digitali. In riferimento alla funzione degli applicativi questi possono essere distinti in: sistemi usati per gestire il personale[172]; *software* utilizzati per fornire spazi virtuali di collaborazione[173]; sistemi impiegati per amministrare i clienti e da cui possono essere tratte informazioni indirette sull'operato dei lavoratori[174]. Si procederà ad una sintetica analisi dei differenti applicativi al fine di comprenderne l'operatività.

3.1. HRIS *(Human Resources Information System).*

I dati utilizzati per la gestione dei lavoratori sono normalmente estratti dal sistema informativo dedicato alle risorse umane denominato *Human Resources Information System* (HRIS)[175] e integrati con i risultati di sondaggi o questionari rivoti ai dipendenti[176]. HRIS è definito come un sistema utilizzato per acquisire, conservare e analizzare informazioni riguardanti le risorse umane di un'organizzazione.

Originariamente, i sistemi HRIS erano distinti da altri applicativi utilizzati dell'impresa e destinati a seguire esclusivamente i processi inerenti alle risorse umane. Con l'avvento della digitalizzazione, i sistemi di HRIS si sono ampliati e integrati con altri *software* in uso presso le aziende, consentendo di gestire un maggior numero di funzioni relative al personale e di

172 HRIS (*Human Resources Information System*)
173 Denominati *Digital workplace*
174 CRM (*Customer Relationship Management*)
175 Esempi di HRIS sono il software Ecosagile; Cornerstone; Monday.com; Workday; Fluida.
176 ANGRAVE D., CHARLWOOD A., KIRKPATRICK I., LAWRENCE M., STUART M., *HR and Analytics: Why HR Is Set to Fail the Big Data Challenge,* in Human Resource Management Journal, vol. 26, no. 1, 2016, 1–11.

offrire applicazioni più sofisticate per le operazioni manageriali e decisionali (per esempio in riferimento al *reporting*). Oggigiorno, i sistemi di HRIS si integrano con le *suite software* ERP (*Enterprise Resource Planning*)[177], un applicativo utilizzato per gestire le attività quotidiane dalle imprese in riferimento al *business*, alla contabilità, al *project management* e al *performance management*. Una *suite* ERP aiuta a pianificare, quantificare, prevedere e comunicare i risultati finanziari di un'organizzazione combinandoli con i dati delle risorse umane. I sistemi HRIS diventano, così, sempre più abilitati al *web* e basati su un'architettura *Internet*. Ciò consente di centralizzare tutti i dati del personale, rendendo possibile accedervi in qualsiasi momento/luogo tramite un *browser web*. Con la digitalizzazione avviene anche un aumento di attenzione ai sistemi di supporto alle decisioni e di *Business Intelligence* (BI)[178] che vengono ulteriormente implementati all'interno dei sistemi di HRIS, consentendo maggiori capacità di analisi. Un HRIS è, quindi, un Sistema Informativo delle Risorse Umane composto da diversi componenti *software* (detti moduli) che, grazie anche all'Intelligenza Artificiale, automatizzano le attività specifiche di ogni processo di gestione di lavoratori come la gestione del lavoro e degli orari, i salari e le retribuzioni, la valutazione delle prestazioni, la mappatura delle competenze ("*soft skill*")[179], la formazione reclutamento e molto altro. Tali dati possono essere centralizzati per elaborare un monitoraggio degli obiettivi raggiunti, per ottenere un reclutamento più efficace ed elaborare previsioni sullo sviluppo di carriera dei lavoratori.

La diffusione di HRIS determina, così, la creazione di grandi quantità di dati sui lavoratori organizzati in *database* che possono essere impiegati quali *set* di dati su cui addestrare o far operare un sistema di IA.

3.2. *Digital Workplace.*

Per *Digital Workplace*[180] si intendono quei *software* "collaborativi" che costituiscono dei veri e propri "spazi di lavoro digitale" all'interno dei quali viene svolta non solo la prestazione lavorativa, ma si sviluppano anche le dinamiche relazionali tra lavoratori e tra questi e

---

177 Un ERP è un sistema completo che integra tutte le funzioni essenziali per la gestione di un'azienda (Contabilità, Inventario e Gestione degli ordini, Risorse Umane, Gestione delle relazioni con i clienti, Produzione, Catena di fornitura, Servizi, Approvvigionamento, etc) e che è in grado di automatizzare ed informatizzare i processi e le informazioni dell'intera organizzazione. Per un esempio di software ERP è si veda in www.fluentis.com.

178 La *Business Intelligence* combina *business analytics*, *data mining*, visualizzazione dei dati, strumenti e infrastrutture per i dati, nonché le *best practice* per permettere alle organizzazioni di prendere più decisioni basate sui dati (si veda in *www.tableau.com*).

179 Cfr. BROLLO M., *Disciplina delle mansioni (art. 3)*, in CARINCI F. (a cura di), *Commento al D. Lgs. 15 giugno 2015, n. 81: le tipologie contrattuali e lo jus variandi,* ADAPT University Press, ADAPT Labour Studies e-Book series, 2015, n. 48, 29-34; CARUSO B., *Strategie di flessibilità funzionale e di tutela dopo il Jobs Act: fordismo, post fordismo e industria 4.0,* in *DLRI,* n. 1, 2018, 81 ss; BENADUSI L., MOLINA S., *Le competenze. Una mappa per orientarsi*, Fondazione Agnelli, Il Mulino, Bologna, 2018.

180 Esempi di *digital workplaces* sono Microsoft 365, Google Suite, Microsoft Viva.

l'organizzazione. Un ambiente di lavoro digitale è una forma virtuale del tradizionale ambiente d'ufficio fisico, in cui molti elementi di collaborazione e produttività vengono eseguiti attraverso una combinazione di applicazioni digitali, *cloud computing* e connettività alla rete. Il termine fa, dunque, riferimento all'ampio ecosistema delle tecnologie sul posto di lavoro. L'ambiente di lavoro digitale rappresenta una piattaforma interattiva di connessione che raccoglie tutti gli strumenti necessari ai lavoratori digitali per svolgere la prestazione e per sviluppare gli obiettivavi dell'organizzazione. Una *Digital Workplace* include molteplici applicativi e strumenti collaborativi quali *app* di comunicazione e messaggistica, programmi di archiviazione *cloud*, piattaforme *intranet* aziendali, sistemi di gestione contenuti e condivisione documenti. La *Digital Workplace* crea, così, un *hub*[181] centralizzato (ovvero una rete informatica) in cui i lavoratori possono accedere alle informazioni e svolgere le proprie attività lavorative, indipendentemente dalla loro ubicazione o dal dispositivo utilizzato.

I più recenti spazi di lavoro digitali[182] sono integrati con ulteriori funzionalità. I lavoratori, accedendo con il proprio *ID* personale alla *Digital Workplace*, possono connettersi all'azienda, trovando comunicazioni interne e risorse aziendali, ma anche ai colleghi, partecipando alle "*community*" composte da gruppi di lavoro. La *Digital Workplace* consente di impostare una relazione integrata e condivisa dall'azienda creando automaticamente dei "*topics*", ovvero delle schede di argomenti all'interno di conversazioni o documenti condivisi sulla piattaforma[183]. La *Digital Workplace* è anche in grado di offrire ai dipendenti (a secondo del ruolo e della funzione ricoperta) approfondimenti e formazione personalizzata, resi maggiormente accessibili in ragione del flusso di lavoro di ogni soggetto[184]. Viene, così, implementata la formazione *E-learning* e *blended learning*[185] volta a creare un percorso di approfondimento personalizzato e, altresì, capace di monitorare l'efficacia delle nozioni apprese da ogni soggetto. Le potenzialità della piattaforma digitale sono orientate anche a favorire la salute dei lavoratori, aiutando a bilanciare occupazione e tempi di riposo[186]. La

[181] Intendendo per *hub* un dispositivo per connettere più elaboratori a una rete e più reti fra loro. Su "dizionari del Corriere" visionabile su *https://dizionari.corriere.it/dizionario_italiano/H/hub.shtml*.

[182] Come Microsoft Viva.

[183] In base ai *topics*, selezionando la scheda desiderata è possibile, in tal modo, accedere a tutti i documenti correlati all'argomento, alle conversazioni inerenti, ai video pertinenti e alle persone coinvolte.

[184] Questa funzionalità aggrega tutte le risorse di apprendimento disponibili per un'azienda in un unico luogo. Dai corsi di formazione tradizionali ai contenuti di micro-apprendimento, gli utenti possono scoprire, condividere, assegnare e monitorare una grande varietà di *training* come parte naturale della giornata lavorativa.

[185] Per *blended learning* si intende un approccio formativo che unisce elementi della formazione tradizionale in presenza con attività *online* guidate da un formatore. A differenza dell'E-*learning*, le lezioni *online* non sostituiscono completamente quelle "analogiche". La tecnologia viene, quindi, impiegata per arricchire l'esperienza formativa. Cfr. TIETZ CAZERI G., DE SANTA-EULALIA L. A., PAVAN SERAFIM M, ANHOLON R., *Training for Industry 4.0: a systematic literature review and directions for future research,* in *Brazilian Journal of Operations & Production Management*, vol. 19, n. 3, 2022, 1-19.

[186] La *Digital Workplace* può, per esempio, pianificare in maniera specifica gli intervalli di lavoro idonei per ottimizzare concentrazione, apprendimento e benessere dei singoli.

piattaforma può anche intervenire per fornire suggerimenti "relazionali" personalizzati proponendo strategie per rafforzare i rapporti con i propri colleghi. Il sistema è, inoltre, abilitato a supportare i *manager* nell'organizzare l'attività lavorativa, rilevando i *trend* (di singoli o gruppi di lavoratori) così da migliorare il bilanciamento tra produttività e il benessere.

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

3.3. CRM (*Customer Relationship Management*).

Il concetto di *Customer Relationship Management* (*CRM*) è legato alla gestione delle relazioni con i clienti di un'impresa. Il *CRM* è una tecnologia basata su *cloud* impiegata per registrare, analizzare e creare *report* delle connessioni attuate dall'azienda con i clienti al fine di migliorare il servizio offerto e "fidelizzare" gli utenti. Il *software CRM* è in grado di registrare informazioni di contatto sui clienti[187], indicazioni sulle preferenze di erogazione del servizio, *feedback* sulle prestazioni ricevute e sul grado di soddisfazione[188]. Nel caso, per esempio, di un *CRM* definito "collaborativo", questo monitora la gestione dei contatti con i clienti mediante gli strumenti di comunicazione aziendali (quali telefono o *e-mail*). Il sistema è, così, in grado si riportare anche il *feedback* sulle attività svolte dai dipendenti per raggiungere tale scopo.

Dai *CRM* è, quindi, possibile trarre informazioni in relazione all'obiettivo o al risultato conseguito dai lavoratori, intesi come *outcome*[189] dell'attività oppure come *output*[190]. Tali sistemi sono, dunque, in grado di fornire *report* "indiretti", ma precisi, sull'attività lavorativa compita dai singoli dipendenti in relazione alle operazioni svolte con i clienti.

4. Interventi dell'AI Act e tutele dei lavoratori. In particolare: la trasparenza dei sistemi di IA.

Dalla ricognizione compiuta nel capitolo precedente sui sistemi di IA impiegati in contesti di lavoro si evince come la transizione digitale delinei una realtà tecnologica dotata di

---

187 Come indirizzo *e-mail,* numero di telefono, profilo sui *social media.*

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

189 Concepito, per esempio, quale ammontare di fatturato conseguito in una determinata zona geografica.

190 Rappresentato dalla quantità di attività svolta dal dipendente come può essere il numero di contatti intrattenuto con i clienti.

innovative capacità di analisi e di altrettante potenzialità di acquisire informazioni originariamente ignote.

Gli interventi introdotti dall'AI Act cercano così di mitigare gli effetti negativi che potrebbero derivare dal "potere tecnologico" che discende dei dati e dalla loro elaborazione.

Capacità che divengono manifestazione di possibili squilibri tra le parti coinvolte nel rapporto, soprattutto ove i lavoratori ignorino l'impiego di strumenti basati su sistemi di IA e le potenzialità di analisi intrinseche a tale tecnologia.

La tecnologia sui dati implementa, dunque, la propria forza in maniera direttamente proporzionale alla mancata trasparenza con cui si manifesta. Questa ambiguità può derivare dalla complessità dei sistemi di IA utilizzati, dalla mancata trasparenza nelle modalità di raccolta e trattamento dei dati, nonché dalla difficoltà per i lavoratori di comprendere come vengono sfruttate le informazioni.

L'opacità dei sistemi di IA può giungere anche dalla tipologia di dati acquisiti che, ove "non autoevidenti", possono celare – dietro un'apparente neutralità – una pluralità di informazioni significative.

Conseguentemente, se i lavoratori ignorano come avvenga la raccolta e l'elaborazione dei dati o non sono in grado di comprendere le informazioni fornite a riguardo, i datori di lavoro possono sfruttare tale *vulnus* per esercitare un controllo disumano (ovvero integralmente delegato alla macchina)[191]. Da qui ne discende la necessità di una tutela che possa porre limiti efficaci al "potere tecnologico" abilitato dai sistemi di IA.

Il principio di trasparenza può contrastare l'intensità di tale potere – rendendo palese nel suo manifestarsi – e ricoprendo un ruolo abilitante dei diritti dei lavoratori: la conoscenza è il presupposto per attivare la salvaguardia degli interessati.

Su tali aspetti interviene il nuovo Regolamento.

AI Act prevede in merito che il *deployer*/datore di lavoro, una volta acquisito un sistema di IA, compia una Valutazione d'Impatto[192] al fine di mappare i rischi connessi all'impiego di tali sistemi e verifichi che trattamento compiuto dall'IA sui dati dei lavoratori rispetti i principi richiesti dall'art. 5 del GDPR. Connessi a ciò, sono rilevanti i doveri di informazione

[191] Diretta conseguenza di ciò è non solo la violazione della libertà di autodeterminazione informativa dei lavoratori, ma anche l'inconsapevole soggezione degli stessi a trattamenti arbitrari o discriminatori. La questione viene sollevata anche da Marco Peruzzi, il quale osserva che l'utilizzo di sistemi di intelligenza artificiale da parte del datore di lavoro può addurre principalmente a due problematiche: da un lato l'aumento del rischio di violazioni dei diritti di conosciuti al lavoratore, dall'altro la difficile individuazione e dimostrazione di detta violazione. In merito si rinvia PERUZZI M., *Intelligenza Artificiale e lavoro. Uno studio su poteri datoriali e tecniche di tutela*, Giappichelli Editore, Torino, 2023, 7 ss.

[192] Ex art. 35 del GDPR.

e consultazione che AI Act impone in capo ai *deployer* prima della messa in servizio o dell'impiego di un sistema di IA nel luogo di lavoro.

I datori di lavoro devono, in primo luogo, rispettare il diritto di informazione e spiegazione di cui sono destinatari i lavoratori (o candidati tali) esposti all'uso di sistemi di IA da cui possano derivare effetti giuridici che li interessino in modo significativo. Tale diritto si traduce in un corrispondente dovere informativo, analogo a quello previsto dal GDPR, che renda note in maniera chiara le finalità per cui è impiegato il sistema di IA, il ruolo da questa svolto nel processo decisionale, i criteri adottati e i dati acquisiti per giungere alla decisione.

AI Act prevede, inoltre, che i datori di lavoro si interfaccino anche con i rappresentanti dei lavoratori. Particolare attenzione è, dunque, posta dal Regolamento alla dimensione superindividuale del principio di trasparenza, individuando nella partecipazione collettiva dei lavoratori una possibile contromisura al "potere tecnologico" dei sistemi di IA. Il coinvolgimento dei lavoratori nella salvaguardia dei dati e il loro intervento anche su aspetti programmatici (come la pianificazione condivisa in merito all'introduzione di tecnologie digitali in contesti lavorativi), può garantire una tutela più efficiente e sicura, agevolando una migliore comprensione delle informazioni fornite. Infatti, ove la forza del "potere tecnologico" dei sistemi di IA derivi dall'accesso ai dati e alle informazioni da questi desumibili mediante l'elaborazione, deve potersi contrapporre un egual potere che ne limiti gli abusi favorendo l'intelligibilità dei sistemi. Bilanciamento che può risultare inefficace ove l'azione di contrasto sia rimessa ai singoli prestatori, ma che può essere garantito dalla tutela collettiva.

La tecnologia potrebbe, così, tutelare i lavoratori coinvolti supportandoli nel percorso informativo e conoscitivo dei sistemi di IA[193]. Tali previsioni, volte a sviluppare tecniche di analisi secondo un approccio realmente antropocentrico, auspicano uno sviluppo e un impiego di IA non più definibili come "*People Analytics*" bensì quali "*Analytics for People*", ossia orientato non ad analizzare la persona, ma di analizzare per la persona.

[193] Potrebbero, per esempio essere predisposti degli *allert* che segnalino l'acquisizione di dati personali e/o particolari dei lavoratori a seguito dell'elaborazione e ponendo in evidenza le finalità per cui l'analisi è stata programmata.
Gli stessi processi automatizzati potrebbero, inoltre, provvedere ad un immediato "oscuramento" delle informazioni sensibili acquisite a seguito dell'elaborazione, adottando tecniche di anonimizzazione, nonché informare tempestivamente gli interessati (o i loro rappresentanti) sulla natura dei dati acquisiti.
Ciò al fine di favorire una valutazione sulla necessità, o meno, di condividere tali informazioni con il datore di lavoro in riferimento alle esigenze di osservazione dichiarate.

DALL'INFORMAZIONE AL COINVOLGIMENTO DELLE PARTI SOCIALI: LA DIMENSIONE COLLETTIVA NEL PRISMA DELL'INTELLIGENZA ARTIFICIALE

Ilaria Purificato
Assegnista di ricerca in Diritto del Lavoro nell'Università degli Studi di Modena e Reggio Emilia - Fondazione Marco Biagi

SOMMARIO: 1. Introduzione. - 2. Gli spazi di intervento degli attori collettivi secondo l'art. 26 del Regolamento IA. - 2.1. Le "informazioni" del Regolamento IA. - 2.1.1. Il "diritto minimo" all'informazione per i lavoratori e i rappresentanti dei lavoratori. - 2.1.2. I diritti di informazione e consultazione. - 2.1.3. Il coinvolgimento dei soggetti collettivi nelle procedure ad oggetto "particolare" nei contesti lavorativi che utilizzano i sistemi di IA. - 2.2. Valutazione d'impatto sulla protezione dei dati. - 3. Valutazione d'impatto sui diritti fondamentali: un'occasione persa per il coinvolgimento degli attori collettivi? - 4. Sorveglianza e riesame umani. - 5. Conclusioni.

1. Introduzione.

L'entrata in vigore del Regolamento (UE) 2024/1689 che stabilisce regole armonizzate sull'intelligenza artificiale (d'ora in avanti Regolamento IA) offre l'occasione per continuare a riflettere sul ruolo degli attori collettivi negli ambienti di lavoro "reali" e "virtuali" in cui vengono utilizzati sistemi di Intelligenza Artificiale (IA)[194].

L'implementazione di tali sistemi nelle tecnologie adottate in azienda e nei processi che determinano il funzionamento delle piattaforme digitali di lavoro ha contribuito allo sviluppo dei cc.dd. sistemi di *management* algoritmico, che progressivamente hanno fagocitato le prerogative datoriali e acquisito la gestione delle fasi di selezione e di assunzione dei lavoratori, acuendo la preesistente asimmetria informativa e lo squilibrio di poteri fisiologicamente esistente tra le parti del rapporto di lavoro[195].

---

194 Si vedano, tra gli altri, CIUCCIOVINO S., *La disciplina nazionale sulll'utilizzazione dell'intelligenza artificiale nel rapporto di lavoro*, in *Lavori Diritti Europa*, 1, 2024; ZAPPALÀ L., *Intelligenza artificiale, sindacato e diritti collettivi*, in BIASI M. (a cura di), *Diritto del lavoro e intelligenza artificiale*, Giuffré, Milano, 2024, 173 ss.; PERUZZI M., *Intelligenza artificiale e lavoro. Uno studio su poteri datoriali e tecniche di tutela*, Giappichelli, Torino, 2023; PURIFICATO I., SENATORI I., *The Position of Collective Rights in the "Platform Work" Directive Proposal: Commission v Parliament*, in *Hungarian Labour Law e-Journal*, 1, 2023, 1-19; SENATORI I., *EU Law and Digitalisation of Employment Relations*, in *GYULAVÀRI, MENEGATTI (eds), Decent Work in the Digital Age. European and Comparative Perspectives, Hart-Bloomsbury, New York, 2022,* 75-76; IMBERTI L., *Intelligenza artificiale e sindacato. Chi controlla i controllori artificiali?*, in *federalismi.it*, 2023, n. 29, 192 ss.; GAUDIO G., *Algorithmic management, sindacato e tutela giurisdizionale*, in *Diritto delle Relazioni Industriali*, 2022, n. 1, 30 ss.; FORLIVESI M., *Interessi collettivi e rappresentanza dei lavoratori del web,* in TULLINI P. (a cura di), *Web e lavoro. Profili evolutivi e di tutela*, Giappichelli, 2017, 192 ss.

195 PERUZZI M., *Intelligenza artificiale, poteri datoriali e tutela del lavoro: ragionando di tecniche di trasparenza e poli regolativi*, in *Ianus*, 2021, n. 24; TULLINI P., *La questione del potere nell'impresa. Una retrospettiva lunga mezzo secolo*, in *Lavoro e Diritto*, 2021, 3-4, 429 ss.

Una tal condizione, accrescendo la necessità di tutele collettive, dovrebbe costituire il presupposto per interventi finalizzati al consolidamento dei soggetti collettivi, in termini tanto di rappresentatività, quanto di coinvolgimento in azienda e di potere negoziale. In altre parole, dovrebbe favorire il rilancio e il consolidamento di tecniche di tutela – anche già disciplinate dalla legge e/o dalla contrattazione collettiva –, in grado di controllare e di ingerirsi sull'esercizio dei poteri datoriali, fronteggiandone eventuali derive, a partire dalle procedure di informazione e consultazione per arrivare a più "forti" diritti di partecipazione, passando per i doveri di trasparenza e informazione.

Tuttavia, è su questo terreno che si scontrano, da una parte, i principi e gli indirizzi elaborati nei documenti di *policy* e negli accordi collettivi e dall'altra, le criticità che si frappongono alla piena realizzazione degli stessi, a partire dall'intreccio tra l'ormai consolidato calo dei tassi di sindacalizzazione e diversi fattori che spingono nella direzione opposta al perseguimento di una sintesi degli interessi collettivi, come il "processo di atomizzazione della prestazione"[196], le logiche della concorrenza e della costruzione di profili reputazionali e l'assenza di spazi fisici o virtuali di aggregazione, per citarne alcuni.

Difatti, molteplici sono ormai i documenti e gli atti di matrice europea in cui si afferma tutta l'importanza del coinvolgimento dei lavoratori e dei loro rappresentanti, ai diversi livelli, nei contesti lavorativi in cui si fa ricorso a sistemi di IA. Come chiaramente indicato nel "Libro Bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia"[197], in cui vengono delineate le strategie dell'Unione Europea per uno sviluppo "affidabile" e "sicuro" dell'IA, "i lavoratori e i datori di lavoro sono interessati direttamente dalla progettazione e dall'uso dei sistemi di IA sul luogo di lavoro" e, dunque, il coinvolgimento delle parti sociali rappresenta "un fattore cruciale per garantire un approccio antropocentrico all'IA sul lavoro".

Le stesse parti sociali europee individuano nell'attivazione di un processo dinamico circolare comune l'approccio più adatto a catturare i vantaggi traghettati dalla digitalizzazione, mitigandone i rischi, e a perseguire un costante contemperamento tra gli interessi dei lavoratori e dei datori di lavoro[198].

Che quella del coinvolgimento dei soggetti collettivi debba essere la via da prediligere per garantire migliori condizioni di lavoro in contesti innovativi e digitalizzati lo confermano

196 FORLIVESI M., *La rappresentanza e la sfida del contropotere nei luoghi di lavoro*, in *Lavoro e Diritto*, 2020, 4, 673 ss.
197 Commissione europea, Bruxelles, 19.2.2020, COM(2020) 65 final.
198 Il riferimento è all' European Social Partners Framework Agreement on Digitalisation. Per approfondimenti, si vedano, tra gli altri, SENATORI I., *The European Framework Agreement on Digitalisation: a Whiter Shade of Pale?*, in *Italian Labour Law e Journal*, 2, 13, 2020, 160-175; BATTISTA L., *The European Framework Agreement on Digitalisation: a tough coexistence within the EU mosaic of actions*, in *Italian Labour Law e Journal*, 1, 14, 2021, 105–121; ROTA A., *Sull'Accordo quadro europeo in tema di digitalizzazione del lavoro*, in *Labour & Law Issues*, 2020, n. 2, 25 ss.

anche alcuni recenti studi condotti a livello europeo, che colgono una relazione positiva tra la presenza di forme di rappresentanza dei lavoratori in aziende in cui siano presenti tecnologie che implementano l'IA e la sussistenza di migliori condizioni di lavoro[199].

Al contempo non si possono sottovalutare e dimenticare le note vicende che hanno connotato le relazioni sindacali del settore del *food delivery* a livello nazionale, dove i movimenti di base costituitisi in risposta alle iniziali assenza e difficoltà delle organizzazioni sindacali di intercettare i lavoratori delle piattaforme digitali e di farsi portavoce dei loro bisogni, hanno agito in luogo degli attori tradizionali o affiancandoli[200].

In considerazione della maggiore esigenza di tutele collettive che si può configurare nei contesti lavorativi in cui il datore di lavoro ricorre all'utilizzo di sistemi di IA, il presente Capitolo ha l'obiettivo di individuare il ruolo e le modalità di intervento riconosciuti dal legislatore europeo agli attori collettivi, a partire da un'analisi delle disposizioni del Regolamento IA.

Difatti, nonostante, come più volte precisato nelle pagine di questo Volume, la base giuridica – artt. 16 e 144 TFUE – lo configuri come strumento di armonizzazione del mercato interno in materia di "protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale", il suddetto Regolamento persegue l'obiettivo di monitorare, valutare e minimizzare i rischi connessi all'uso di sistemi di IA anche nel settore dell' "occupazione, gestione dei lavoratori e accesso al lavoro autonomo", riconoscendo agli attori collettivi, quali possibili *stakeholder*, spazi di intervento funzionali a garantire il rispetto della trasparenza[201] in appositi segmenti della catena del valore dell'IA.

Sul piano del metodo, l'analisi prende le mosse dall'articolato del Regolamento IA per poi avviare un dialogo con quelle fonti, europee e nazionali, che, come osservato più volte nel presente Volume[202], costituiscono le tessere di un medesimo mosaico. Nello specifico, i riferimenti sono al Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche

---

[199] CAZES S., *Social dialogue and collective bargaining in the age of artificial intelligence*, in *OECD Employment Outlook 2023 artificial intelligence and the labour market*, 221 ss.

[200] Si vedano, MARRONE M., *Rights against the machines! Food delivery, piattaforme digitali e sindacalismo informale*, in *Labour & Law Issues* 5, 1, 2019, I.3 ss.; PACELLA G., *Le piattaforme di food delivery in Italia: un'indagine sulla nascita delle relazioni industriali nel settore*, in *Labour & Law Issues,* 5, 2, 2019, 181 ss.; MARTELLONI F., *Individuale e collettivo: quando i diritti dei lavoratori digitali corrono su due ruote*, in *Labour & Law Issues* 4, 1, 2018, 18 ss.; TASSINARI A., MACCARONE V., *Riders on the storm. Workplace solidarity among gig economy couriers in Italy and the UK*, in *Work, Employment and Society,* 2019; PURIFICATO I., SCELSI A. con la supervisione di Senatori I., Spinelli C., *Representing and Regulating Platform Work: Emerging Problems and Possible Solutions. National report on Italy*, 41-52, https://irel.fmb.unimore.it/archive/research-output/national-reports/.

[201] Sulle due diverse accezioni di trasparenza nell'ambito del Regolamento IA, si veda in questo Volume, PALMIROTTA F., *Il Regolamento IA nel sistema del Diritto del lavoro: verso la regolazione del management algoritmico,* 40.

[202] Si vedano, in questo Volume, SENATORI I., *Introduzione. L'AI Act: un nuovo tassello nella Costruzione dell'ordinamento del lavoro digitale*, 10 ss. e, PALMIROTTA F., *Il Regolamento IA nel sistema del Diritto del lavoro*, cit. 28 ss.

con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (d'ora in avanti, GDPR), alla Proposta di Direttiva relativa al miglioramento delle condizioni di lavoro nel lavoro mediante piattaforme digitali (d'ora in avanti Direttiva sul lavoro mediante piattaforme digitali), nonché a delle disposizioni del nostro ordinamento il cui ambito di applicazione riguarda processi e tecnologie che possono integrare sistemi di IA, quali l'art. 1-bis del d. lgs. n. 152/1997[203] e l'art. 4 dello Statuto dei Lavoratori[204]. L'interrogazione sinergica di tali fonti è essenziale perché, come chiarito da Federica Palmirotta nel Capitolo III di questo Volume, le nozioni di "trattamento automatizzato" e di "sistemi automatizzati di decisione e monitoraggio" non coincidono necessariamente con quella di sistema di IA, ma possono fare riferimento a sistemi che integrano una tecnica di IA, così come la nozione di "strumento di controllo a distanza" può includere quella di sistema di IA, nei casi in cui quest'ultimo venga impiegato per monitorare il lavoratore.

2. Gli spazi di intervento degli attori collettivi secondo l'art. 26 del Regolamento IA.

La prima delle poche disposizioni del Regolamento IA che rilevano ai fini della nostra analisi è l'articolo 26, rubricato "Obblighi dei *deployer* dei sistemi di IA ad alto rischio", in cui il monitoraggio costante del funzionamento dei sistemi di IA da parte delle persone fisiche, la trasparenza e la previsione di misure di responsabilizzazione del *deployer* vengono individuati come strategie per fronteggiare i rischi per la sicurezza e i diritti fondamentali degli individui che l'utilizzo di tali sistemi può sollevare. Tali finalità, nell'ambito del nostro specifico settore di indagine, possono considerarsi essenzialmente rimesse dall'art. 26 a due strumenti, che prevedono anche l'intervento degli attori collettivi: l'informazione e la valutazione d'impatto sulla protezione dei dati.

2.1. Le "informazioni" del Regolamento IA.

L'art. 26, al paragrafo 7 disciplina gli obblighi del *deployer* nell'ipotesi in cui questo utilizzi o voglia utilizzare i sistemi di IA ad alto rischio – così come individuati nell'allegato III, n. 4 del documento – sul luogo di lavoro.

La suddetta disposizione pone in capo al datore di lavoro-*deployer* un obbligo di

[203] D. Lgs 104/2022, così come da ultimo modificato dal c.d. Decreto Lavoro (D.L. n. 48/2023). Si vedano, tra i tanti, FAIOLI M., *Trasparenza e monitoraggio digitale. Perché abbiamo smesso di capire la norma sociale europea,* in *federalismi.it*, 2022, 25; contra 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 poteridatoriali algoritmici?*, in *Labor*, 2023, 1, 11 ss.; ZILLI A., *Condizioni di lavoro (finalmente) «trasparenti e prevedibili»,* in *Labor*, 6, 2022.
[204] L. n. 300/1970.

informazione circa l'uso di sistemi di IA ad alto rischio nei confronti dei rappresentanti dei lavoratori e degli stessi lavoratori, chiarendo che "tali informazioni sono fornite, se del caso, 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".

Una formulazione ben diversa da quella presentata nella versione emendata dal Parlamento europeo che, al paragrafo 5a, dell'allora art. 29, da una parte, richiamava espressamente l'obbligo per il *deployer* di avviare, prima dell'utilizzo del sistema di IA, le procedure di informazione e consultazione dei rappresentanti dei lavoratori di cui alla direttiva 2002/14/CE, dall'altra disponeva che, una volta che quest'ultimo fosse entrato in funzione, tutti i lavoratori interessati dal suo operare avrebbero dovuto ricevere adeguata informazione.

Dal confronto appare evidente, in primo luogo, che ogni riferimento puntuale alla normativa vigente scompare nel testo approvato, lasciando spazio ad un più generale rinvio alle "norme e alle procedure stabilite dal diritto e dalle prassi dell'Unione e nazionali". Tale opzione consentirebbe di estendere la portata dell'obbligo informativo oltre le direttive ad oggetto "generalista", finendo per includere anche le direttive ad oggetto "particolare", segnatamente quelle in materia di salute e sicurezza sui luoghi di lavoro[205], nonché di licenziamenti collettivi[206].

In secondo luogo, si assiste alla fusione del diritto di informazione e consultazione e del diritto di informazione in un indefinito obbligo di informazione per il *deployer* da assolvere, a seconda dei casi, alternativamente o cumulativamente nei confronti dei rappresentanti dei lavoratori e dei lavoratori.

In verità, tale obbligo informativo, come si evince dalla lettura del considerando n. 92, oltre a sintetizzare il riferimento ai due distinti diritti appena citati, pare introdurre un obbligo per il datore di lavoro di informare tanto i lavoratori quanto i rappresentanti dei lavoratori circa la "diffusione programmata dei sistemi di IA ad alto rischio sui luoghi di lavoro" al fine di tutelare i diritti fondamentali sanciti nella Carta dei diritti fondamentali dell'Unione Europea.

Tuttavia, a tale obbligo dovrebbe riconoscersi natura residuale in quanto il *deployer* è tenuto a ottemperarvi unicamente "laddove non siano soddisfatte le condizioni per [gli] obblighi di informazione o di informazione e consultazione previsti da altri strumenti giuridici". Ciò equivarrebbe ad affermare la costituzione di un "diritto minimo", a titolo esemplificativo,

[205] Si veda, PERUZZI M., *Sistemi automatizzati e tutela della salute e sicurezza sul lavoro*, in *Diritto della Sicurezza sul Lavoro*, 2024, 2, 91-92.
[206] V. infra par. 2.1.3.

per i lavoratori e i rappresentanti dei lavoratori delle imprese e degli stabilimenti che non raggiungono i requisiti dimensionali minimi previsti dalla direttiva 2002/14/CE ai fini della sua applicabilità o, ancora, per i lavoratori autonomi, quantomeno nella fase di accesso al lavoro, se si considera che la definizione di sistemi di IA ad alto rischio di cui all'allegato III, al n. 4 include il settore dell'"occupazione, [della] gestione dei lavoratori e [dell'] accesso al lavoro autonomo", nonché nelle fasi di selezione e assunzione.

La scelta operata nell'art. 26, par. 7, del Regolamento IA di "appiattire" i diversi strumenti sembra tener conto solo delle affinità e non delle differenze che sussistono tra gli stessi, quantomeno dal punto di vista delle funzioni dagli stessi svolte.

Applicando il filtro della differenza, difatti, le informazioni dovrebbero distinguersi tra quelle la cui finalità esclusiva (almeno apparentemente) è la conoscenza degli aspetti che hanno guidato il datore nell'esercizio dei suoi poteri e quelle che comportano un vero e proprio coinvolgimento dei rappresentanti dei lavoratori[207].

Nella prima ipotesi, si sarebbe in presenza di un "semplice" dovere di informazione funzionale a garantire un controllo sull'esercizio del potere datoriale, in questi casi espresso dal *management* algoritmico. Entro tale contenitore rientrerebbero, per affinità, le informazioni da fornire ai lavoratori a cui fa riferimento anche la direttiva (UE) 2019/1152 e le informazioni "minime" da fornire ai lavoratori e ai loro rappresentanti nelle ipotesi "residuali".

Nella seconda categoria di informazioni, invece, sarebbero riconducibili i diritti di informazione e consultazione quali veri e propri strumenti di coinvolgimento dei rappresentanti dei lavoratori nei processi aziendali in grado di "interferire" con l'esercizio unilaterale dei poteri datoriali.

Sebbene la diversità delle funzioni tra gli strumenti appena indicati sia evidente, non si può escludere a priori che anche le "semplici" informazioni che il datore di lavoro è tenuto a fornire ai soggetti collettivi possano avere, in determinate circostanze e se raccordate con altri strumenti, un potenziale (si veda *infra* par. 2.1.1.), spendibile non solo in sede giudiziaria.

2.1.1. Il "diritto minimo" all'informazione per i lavoratori e per i rappresentanti dei lavoratori.

Se il "diritto minimo" di informazione introdotto dal Regolamento IA può presentare

[207] La definizione di coinvolgimento dei rappresentanti dei lavoratori si può far coincidere con quella fornita nella Direttiva 2001/86/CE, che vi include "qualsiasi meccanismo, ivi comprese l'informazione, la consultazione e la partecipazione, mediante il quale i rappresentanti dei lavoratori possono esercitare un'influenza sulle decisioni".

delle affinità con i diritti di informazione in termini di funzione svolta, se ne discosta con riferimento all'ambito soggettivo di applicazione, in quanto, diversamente da quanto previsto nella direttiva in materia di informazione, i suoi destinatari sono tanto i rappresentanti dei lavoratori quanto i lavoratori.

Compiendo tale scelta, il legislatore europeo mantiene una continuità logica innanzitutto tra il Regolamento IA e quanto stabilito nell'art. 9 della proposta di Direttiva sul lavoro mediante piattaforme digitali nella parte in cui dispone che gli Stati Membri debbano imporre alle piattaforme digitali di lavoro di informare le persone che svolgono un lavoro mediante piattaforme digitali e i rappresentanti dei lavoratori delle piattaforme digitali circa l'uso di sistemi automatizzati di decisione e di monitoraggio.

Tale "doppia titolarità del diritto di informazione"[208] contraddistingue anche l'art. 1-bis del d. lgs. n. 152/1997, così come formulato dal c.d. Decreto Trasparenza[209], attuativo della direttiva (UE) 2019/1152 relativa a condizioni di lavoro trasparenti e prevedibili nell'Unione europea, e modificato dal successivo d.l. n. 48/2023, convertito con legge n. 85/2023.

Difatti, l'art. 1-bis pone in capo al datore di lavoro – o al committente pubblico – un obbligo di informazione circa l'utilizzo di sistemi decisionali o di monitoraggio integralmente automatizzati nei confronti dei lavoratori e delle "rappresentanze sindacali aziendali ovvero [de]lla rappresentanza sindacale unitaria e, in assenza delle predette rappresentanze, [de]lle sedi territoriali delle associazioni sindacali comparativamente più rappresentative sul piano nazionale"[210], oltre a riconoscere il diritto di accedere a informazioni ulteriori su richiesta dei lavoratori o delle rappresentanze sindacali aziendali o territoriali, per conto dei lavoratori[211].

Concordando con quanto osservato in dottrina[212], tale obbligo di informazione degli attori collettivi presenta un forte potenziale per l'azione degli stessi soggetti nell'ambito dell'utilizzo dei sistemi di IA e automatizzati, se letto unitamente alle previsioni di cui all'art. 4 dello Statuto dei lavoratori, al quale lo stesso art. 1-bis, nell'ultima parte del par. 1, fa riferimento.

Nello specifico, se gli strumenti che utilizzano sistemi di IA nei luoghi di lavoro e le piattaforme digitali di lavoro sarebbero da qualificare apparentemente come "strumenti di lavoro", è altrettanto vero che l'accesso, da parte dei soggetti collettivi, alle informazioni sul

[208] RECCHIA G.A., *Condizioni di lavoro trasparenti, prevedibili e giustiziabili: quando il diritto di informazione sui sistemi automatizzati diventa uno strumento di tutela collettiva*, in *Labour & Law Issues*, 2023, 1, 44.
[209] D. lgs. 27 giugno 2022, n. 104.
[210] Art. 1-bis, comma 6, del D. lgs. n. 157/1970.
[211] Art. 1-bis, comma 3, del D. lgs. n. 157/1970. Tale strumento è stato largamente utilizzato dal sindacato per avviare una serie di azioni finalizzate ad ottenere la condanna delle piattaforme digitali per non aver fornito adeguate informazioni ai soggetti collettivi in merito ai sistemi automatizzati. Si vedano, Trib. Palermo 31 marzo 2023; Trib. Palermo 20 giugno 2023; Trib. Torino 5 agosto 2023, in DeJure.
[212] RECCHIA G.A., *op. cit.*

funzionamento di tali strumenti potrebbe costituire la chiave di accesso per smentire tale classificazione, laddove gli strumenti appena citati esercitassero anche forme di controllo dei lavoratori, aprendo, di conseguenza, la strada ad una contrattazione con le rappresentanze in azienda per autorizzarne l' utilizzo, conformemente alle previsioni statutarie.

Quanto al contenuto dell'informazione che il *deployer* è chiamato a fornire, all'art. 26, par. 7, del Regolamento IA, non si rinviene alcun riferimento esplicito.

Anche laddove si ritenesse che al datore di lavoro-*deployer* debba trovare applicazione quanto stabilito per il *deployer*-non datore di lavoro, vale a dire il contenuto di cui al paragrafo 11 dell'articolo 26, la lacuna sarebbe colmata solo parzialmente. Difatti, mentre il paragrafo da ultimo citato fa riferimento unicamente ai sistemi di IA ad alto rischio che "adottano decisioni o [che] assistono nell'adozione di decisioni che riguardano le persone fisiche", i sistemi di IA ad alto rischio con un potenziale impatto sul lavoratore possono essere utilizzati per ulteriori finalità, tra cui il monitoraggio[213]. Ne deriva che solo in determinati casi, le informazioni che dovrebbero essere fornite ai lavoratori e ai loro rappresentanti coinciderebbero con le finalità previste dall'utilizzo dell'IA, il tipo di decisioni adottate tramite lo stesso, nonché il diritto che viene riconosciuto alla persona fisica di ricevere una spiegazione. A ciò si aggiunga che anche l'ambito di applicazione del diritto subirebbe una compressione, in quanto il par. 11 dell'articolo che si sta analizzando si riferisce ad un'informazione da fornire unicamente alla persona fisica che è soggetta all'uso di sistemi IA ad alto rischio che adottano o assistono nell'adozione di decisioni che la riguardano.

2.1.2. I diritti di informazione e consultazione.

Venendo al piano dei diritti di informazione e consultazione, come anticipato, nell'attuale formulazione dell'art. 26, par. 7, il riferimento diretto alla Direttiva 2002/14/CE è stato sostituito dal più generico rinvio, "se del caso", 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", con le possibili implicazioni interpretative che *supra* si è visto possono derivarne.

Restando entro i confini della procedura generalista in materia di informazione e consultazione, il "caso" che consentirebbe l'applicazione della Direttiva 2002/14/CE è individuato dalla lett. c), dell'art. 4, par. 2, secondo cui l'informazione e la consultazione riguardano "le decisioni suscettibili di comportare cambiamenti di rilievo in materia di

[213] Anche laddove si opterebbe per un'interpretazione estensiva del termine "decisioni", arrivando a includervi l'assunzione, l'assegnazione di compiti, la cessazione del rapporto di lavoro, il monitoraggio rimarrebbe comunque escluso dall'ambito di applicazione dell'art. 26, par. 11.

organizzazione del lavoro …", fermo il rispetto dei requisiti dimensionali delle imprese di cui all'art.3. Difatti, l'introduzione o la modifica di un sistema di IA nelle tecnologie utilizzate in azienda o nei sistemi automatizzati delle piattaforme digitali può impattare sull'organizzazione del lavoro, modificandola, e per ciò richiedendo l'attivazione delle procedure di informazione e consultazione.

Nella sostanza, ma non nella forma[214], l'approccio adottato dal Regolamento IA coincide con quello della proposta di Direttiva sul lavoro mediante piattaforme digitali, che all'art. 13 rinvia *in toto* la disciplina dei diritti di informazione e consultazione alla Direttiva 2002/14/CE, sia pur introducendo il diritto per i rappresentanti dei lavoratori di farsi assistere da un esperto per esaminare la questione oggetto di informazione e consultazione ed elaborare un parere.

Entrambi gli atti confermano la scelta originariamente compiuta dal legislatore europeo di circoscrivere l'ambito di applicazione dei diritti di informazione e consultazione ai soli rappresentanti dei lavoratori subordinati. Nello specifico, l'art. 26, al par. 7, non include alcuna specifica circa la situazione dei lavoratori autonomi, anch'essi titolari di diritti fondamentali che, in quanto tali, andrebbero tutelati da un utilizzo scorretto dei sistemi di IA ad alto rischio. Ne deriva che tali lavoratori dovrebbero ritenersi titolari del più generico "diritto minimo" a ricevere informazioni.

Chiarita la procedura da applicare e il relativo ambito di applicazione, occorre individuare i contenuti dell'informativa che deve essere fornita ai rappresentanti dei lavoratori affinché si possa dare corretta attuazione ai diritti di informazione e consultazione. In altre parole, ci si interroga sulle informazioni di cui è effettivamente in possesso il *deployer*, che, di conseguenza, potrebbero costituire l'oggetto dell'informativa. In relazione a tali informazioni, talvolta dalla natura estremamente tecnica, ci si può chiedere poi quanto queste possano essere effettivamente comprese dalle rappresentanze dei lavoratori al fine di poter attuare un'utile consultazione.

Per quel che riguarda il primo profilo di indagine, vale a dire l'identificazione delle

[214] La proposta di Direttiva sul lavoro mediante piattaforme ricorre ad un approccio diametralmente opposto a quello adottato dal Regolamento IA in termini di rinvio alla normativa già esistente in materia. Difatti, l'art. 13 dispone che "1.La presente direttiva non pregiudica la direttiva 89/391/CEE per quanto riguarda l'informazione e la consultazione, né le direttive 2002/14/CE e 2009/38/CE.
2. Oltre a rispettare le direttive di cui al paragrafo 1, gli Stati membri provvedono affinché l'informazione e la consultazione, quali definite all'articolo 2, lettere f) e g), della direttiva 2002/14/CE, dei rappresentanti dei lavoratori da parte delle piattaforme di lavoro digitali riguardino anche le decisioni che possono comportare l'introduzione di sistemi decisionali o di monitoraggio automatizzati o modifiche sostanziali al loro utilizzo. Ai fini del presente paragrafo, l'informazione e la consultazione dei rappresentanti dei lavoratori sono effettuate secondo le stesse modalità relative all'esercizio dei diritti di informazione e consultazione previste dalla direttiva 2002/14/CE. …"

informazioni di cui è in possesso il *deployer*, si può ritenere che queste possano essenzialmente coincidere con le istruzioni per l'uso (concise, complete, corrette, chiare e essere pertinenti, accessibili e comprensibili) che il fornitore è tenuto a consegnargli, fatte salve le ulteriori informazioni che potrebbero generarsi nell'ipotesi in cui il *deployer* agisca secondo le modalità di cui all'art. 25, diventando egli stesso un fornitore[215].

Tra le istruzioni alle quali si fa riferimento, secondo quanto disposto dal par. 2, dell'art. 13, vi sono:

"b) le caratteristiche, le capacità e i limiti delle prestazioni del sistema di IA ad alto rischio, tra cui:

i) la finalità prevista;

ii) qualsiasi circostanza nota o prevedibile connessa all'uso del sistema di IA ad alto rischio in conformità della sua finalità prevista o in condizioni di uso improprio ragionevolmente prevedibile che possa comportare rischi per la salute e la sicurezza o per i diritti fondamentali di cui all'articolo 9, paragrafo 2;

iii) se del caso, le capacità e caratteristiche tecniche del sistema di IA ad alto rischio connesse alla fornitura di informazioni pertinenti per spiegarne l'output;

iv) ove opportuno, le sue prestazioni per quanto riguarda le persone o i gruppi di persone specifici sui quali il sistema è destinato a essere utilizzato;

…

d) le misure di sorveglianza umana

f) se del caso, una descrizione dei meccanismi inclusi nel sistema di IA ad alto rischio che consente ai deployer di raccogliere, conservare e interpretare correttamente i log".

Tali informazioni specifiche andrebbero, poi, integrate da quelle che il datore di lavoro è tenuto a fornire ai rappresentanti dei lavoratori secondo quanto stabilito dalla Direttiva 2002/14/CE, in merito alle ricadute organizzative e occupazionali derivanti dall'utilizzo di sistemi di IA.

Si tratta, evidentemente, di informazioni che denotano un elevato grado di complessità e tecnicità, che, se individuate dalla legge o, come si può immaginare per l'Italia, dalla

[215] Art. 25, par. 1: "Qualsiasi distributore, importatore, deployer o altro terzo è considerato fornitore di un sistema di IA ad alto rischio ai fini del presente regolamento ed è soggetto agli obblighi del fornitore a norma dell'articolo 16, nelle circostanze seguenti:
a) se appone il proprio nome o marchio su un sistema di IA ad alto rischio già immesso sul mercato o messo in servizio, fatti salvi accordi contrattuali che prevedano una diversa ripartizione degli obblighi al riguardo;
b) se apporta una modifica sostanziale a un sistema di IA ad alto rischio già immesso sul mercato o già messo in servizio in modo tale che resti un sistema di IA ad alto rischio a norma dell'articolo 6;
c) se modifica la finalità prevista di un sistema di IA, anche un sistema per finalità generali, che non è stato classificato come ad alto rischio e che è già stato immesso sul mercato o messo in servizio in modo tale che il sistema di IA interessato diventi un sistema di IA ad alto rischio a norma dell'articolo 6".

contrattazione collettiva, come informazioni che dovrebbero essere fornite ai rappresentanti dei lavoratori potrebbero minare l'efficacia dell'informazione. Per tali motivi, l'assistenza di esperti, oltre ad una formazione specifica delle stesse rappresentanze e dei lavoratori, appaiono necessarie.

Il Regolamento IA, all'art. 4[216], interviene sul punto, sia pur limitatamente ai lavoratori, stabilendo che i *deployer* debbano garantire un livello sufficiente di alfabetizzazione in materia di IA al loro personale che utilizza i sistemi di IA. Mentre per le rappresentanze dei lavoratori nulla si evince dal Regolamento, demandando apparentemente l'acquisizione di competenze tecniche ad una formazione extra-aziendale

2.1.3. Il coinvolgimento dei soggetti collettivi nelle procedure ad oggetto "particolare" nei contesti lavorativi che utilizzano i sistemi di IA.

La nuova e definitiva formulazione dell'art. 26, par. 7, come anticipato nel par. 2.1., stabilendo che l'informazione dei lavoratori e dei loro rappresentanti debba essere disciplinata dalle "norme e [d]alle procedure stabilite dal diritto e dalle prassi dell'Unione e nazionali in materia" apre la strada ad un'interpretazione estensiva della stessa, tale da potervi includere il riferimento anche alle norme che regolano il coinvolgimento dei lavoratori nelle ipotesi di licenziamento collettivo e nel sistema prevenzionistico.

Relativamente all'articolata disciplina che regola la riduzione del personale, il richiamo alla "cessazione dei rapporti contrattuali" di cui all'allegato III, punto 4, lett. B) del Regolamento IA confermerebbe che questa possa trovare attuazione anche quando la risoluzione del rapporto sia il risultato di una decisione adottata con l'utilizzo di sistemi di IA[217].

Nello specifico, rispettati i requisiti dimensionali e causali richiesti dalla normativa vigente – che plausibilmente potrebbero qualificare i sistemi di IA non solo come "artefici materiali" della decisione, ma anche come motivo che ne è alla base, nelle ipotesi del c.d. licenziamento tecnologico – la procedura prenderebbe avvio con una comunicazione indirizzata ai rappresentanti dei lavoratori in azienda e alle associazioni sindacali e si arricchirebbe dell'eventuale esame congiunto, che potrebbe determinare la chiusura della procedura stessa

[216] Art. 4 Regolamento IA: "I fornitori e i deployer dei sistemi di IA adottano misure per garantire nella misura del possibile un livello sufficiente di alfabetizzazione in materia di IA del loro personale nonché di qualsiasi altra persona che si occupa del funzionamento e dell'utilizzo dei sistemi di IA per loro conto, prendendo in considerazione le loro conoscenze tecniche, la loro esperienza, istruzione e formazione, nonché il contesto in cui i sistemi di IA devono essere utilizzati, e tenendo conto delle persone o dei gruppi di persone su cui i sistemi di IA devono essere utilizzati".

[217] Invece, per il licenziamento per motivi "tecnologici" riconosciuto dall'ILO (Convenzione ILO n. 158 del 1982 sulla cessazione del lavoro) e della giurisprudenza, si vedano, tra gli altri, DE STEFANO V., *"Negoziare l'algoritmo": Automazione, intelligenza artificiale e tutela del lavoro*, in *Occupazione e lavoro, documento di lavoro n.246*, ILO, 2018; Cass. sez. lav. n. 92/2009.

laddove venga raggiunto un accordo tra le parti.

È dall'integrazione tra il Regolamento IA e la normativa prevenzionistica che derivano spazi significativi per l'informazione, la consultazione e la partecipazione dei rappresentanti dei lavoratori – e/o dei lavoratori –[218]. Rientra, difatti, tra gli obblighi generali del datore di lavoro quello di informare i lavoratori e i rappresentanti dei lavoratori dei rischi per la salute e la sicurezza e le misure di prevenzione adottate, ma, come disposto dall'art. 13 della direttiva 89/391/CEE, sussiste anche un più "forte" momento di coinvolgimento per i lavoratori e, per quel che qui interessa, i rappresentanti specializzati dei lavoratori, ponendosi in capo al datore di lavoro l'obbligo di consultare tali soggetti e, conformemente alle norme e/o prassi nazionali, di garantire una partecipazione bilanciata degli stessi su questioni inerenti la salute e la sicurezza del lavoro[219].

Inoltre, come già evidenziato nel presente volume, un ulteriore opportunità di coinvolgimento dei soggetti collettivi verrebbe a configurarsi laddove il sistema di gestione dei rischi, così come pensato all'art. 9 del Regolamento IA, diventi un obbligo a carico del *deployer* che ha agito secondo le modalità di cui all'art. 25, così trasformandosi, per previsione dello stesso articolo, in un fornitore. In tal caso, difatti, la procedura di gestione finirebbe per integrarsi nell'obbligo prevenzionistico, con ciò che ne deriva sul fronte dei ruoli e delle funzioni che dovranno essere svolti dai rappresentanti dei lavoratori "specializzati".

2.2. Valutazione d'impatto sulla protezione dei dati.

Restando nell'ambito delle procedure da avviare *ex ante* rispetto all'utilizzo di sistemi di IA ad alto rischio sul lavoro che coinvolgono anche i rappresentanti dei lavoratori, il Regolamento IA al paragrafo 9 dell'articolo 26 richiama espressamente la valutazione d'impatto sulla protezione dei dati.

Nello specifico, la norma dispone che laddove l'utilizzo di sistemi di IA ad alto rischio comporti il trattamento di dati personali, si costituisce in capo al *deployer* – e, dunque, anche al datore di lavoro – l'obbligo di effettuare, in via preventiva, una valutazione d'impatto sulla protezione dei dati, così come disciplinata dall'art. 35 del Regolamento (UE) 2016/679, in quanto "la natura, l'oggetto, il contesto e le finalità" del trattamento dei dati presentano un rischio elevato per i diritti e le libertà delle persone fisiche[220].

---

218 V. PERUZZI M., *Sistemi automatizzati e tutela della salute e della sicurezza*, cit., 91.

219 Si veda, in particolare, sul tema: ALES E., *La tutela della salute sul lavoro nel prisma del metodo partecipativo*, in ZOPPOLI L. (a cura di), *Tutela della salute pubblica e rapporti di lavoro, Editoriale Scientifica, Napoli, 2021, 231-249;* ID., *La partecipazione (bilanciata) nello Statuto dei Lavoratori: riflessioni sulle rappresentanze ex art. 9, in Diritti Lavori Mercati, 2020, 15-28*.

220 V. Gruppo di lavoro Articolo 29, 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

Nell'ottica della presente analisi, tale strumento di *accountability*, inaugura potenziali spazi per il coinvolgimento dei lavoratori e dei loro rappresentanti dal momento che il par. 9 dell'art. 35 dispone che il titolare del trattamento debba raccogliere le opinioni degli interessati (lavoratori) o dei loro rappresentanti (sindacati) sul trattamento previsto.

Sebbene ad una prima lettura l'art. 35 del GDPR sembri non attribuire carattere vincolante alla raccolta del parere dei soggetti interessati dal trattamento dei dati e dei loro rappresentanti da parte del titolare del trattamento, come chiarito dal Gruppo di lavoro Articolo 29 (WP29), quest'ultimo è tenuto a raccogliere sempre il parere degli interessati, salvo non ritenga che ciò non sia appropriato perché, ad esempio, risulterebbe sproporzionato o impraticabile o potrebbe compromettere la riservatezza dei piani economici dell'impresa. In tal caso, il WP29 spiega che il titolare del trattamento è tenuto a fornire una giustificazione per la mancata raccolta delle opinioni.

Se, dunque, non ricorrono tali circostanze "eccezionali" il titolare del trattamento deve raccogliere le opinioni degli interessati e motivare un eventuale discostamento della sua decisione finale da tali pareri[221].

È evidente che le modalità in cui concretamente si articola la valutazione d'impatto in esame, relativamente al coinvolgimento dei rappresentanti degli interessati dal trattamento dei dati, mostrano dei parallelismi con la procedura di consultazione dei rappresentanti dei lavoratori, ricalcandone i momenti essenziali, quali la raccolta del parere e la motivazione alla base del discostamento della decisione adottata dal parere presentato dagli attori collettivi.

Tale assimilazione è ancora più evidente nella Direttiva sul lavoro mediante piattaforme digitali, che all'articolo 8 dispone l'obbligo per le piattaforme digitali di lavoro, in qualità di titolari del trattamento, di effettuare la valutazione d'impatto sui dati personali ai sensi dell'art. 35 del GDPR, utilizzando espressamente nel considerando n. 44 il termine "consultazione" per indicare le forme del coinvolgimento dei lavoratori e dei loro rappresentanti nell'ambito della procedura in esame[222].

3. Valutazione d'impatto sui diritti fondamentali: un'occasione persa per il coinvolgimento degli attori collettivi?

Con la finalità di garantire la tutela dei diritti fondamentali, l'articolo 27 del Regolamento

(UE) 2016/679, 4 aprile 2017 (come modificate e adottate da ultimo il 4 ottobre).

[221] *Ivi*, 17.

[222] Considerando n. 44 della proposta di Direttiva sul lavoro mediante piattaforme digitali: "Tenendo conto degli effetti che le decisioni prese dai sistemi decisionali automatizzati hanno sulle persone che svolgono un lavoro mediante piattaforme digitali e, in particolare, sui lavoratori delle piattaforme digitali, la presente direttiva stabilisce norme più specifiche relative alla consultazione delle persone che svolgono un lavoro mediante piattaforme digitali e dei loro rappresentanti nel contesto delle valutazioni d'impatto sulla protezione dei dati".

IA introduce una procedura, da applicare al primo utilizzo del sistema di IA ad alto rischio e da aggiornare ogniqualvolta i fattori oggetto di valutazione dovessero subire delle variazioni, che definisce "valutazione d'impatto sui diritti fondamentali".

La finalità principale di tale strumento è quella di individuare i rischi specifici per i diritti fondamentali derivanti dall'utilizzo di tali sistemi di IA, i soggetti o gruppi di soggetti che potrebbero subirne le implicazioni e le misure da attuare nell'ipotesi in cui tali rischi dovessero realizzarsi.

Anche in tale procedura, così come nella valutazione d'impatto sul trattamento dei dati, è previsto un momento di coinvolgimento dei portatori di interessi, che, come specificato nel considerando n. 96, potrebbero essere anche "rappresentanti di gruppi di persone … interessati dal sistema di IA". Tale momento potrebbe coincidere tanto con lo svolgimento della valutazione d'impatto quanto con la progettazione delle misure da attuare nel caso in cui i rischi dovessero realizzarsi.

Chi scrive ritiene che tale valutazione d'impatto si sarebbe potuta candidare come strumento per incrementare il coinvolgimento dei rappresentanti dei lavoratori, se non fosse che il suo ambito di applicazione, ristretto alle organizzazioni di diritto pubblico o enti di diritto privato che forniscono servizi pubblici e ai *deployer* di sistemi di IA ad alto rischio nell'ambito dell' "accesso a servizi privati essenziali e a prestazioni e servizi pubblici essenziali e alla fruizione degli stessi", ne esclude l'applicabilità per i *deployer* che utilizzano i sistemi di IA sui luoghi di lavoro.

Non si giungerebbe ad una soluzione interpretativa diversa neanche considerando la precisazione contenuta nel par. 4, secondo cui la valutazione d'impatto sui diritti fondamentali andrebbe ad integrare la valutazione d'impatto sui dati personali laddove "uno qualsiasi degli obblighi [richiesto ai fini della prima] è già rispettato mediante la valutazione d'impatto sulla protezione dei dati". A parere di chi scrive, diversamente da quanto è stato sostenuto in dottrina, tale previsione non sembra "accorpare" la valutazione di impatto sui diritti fondamentali dei sistemi ad alto rischio alla valutazione d'impatto *ex* art. 35 del GDPR, oltre l'ambito di applicazione previsto nella prima parte dell'articolo.

Gli stessi considerando, come il n. 48, nei quali si fa espressamente riferimento all'impatto che l'uso dei sistemi di IA potrebbero avere sui diritti fondamentali nell'ambito del lavoro, confermerebbero che la scelta operata dal legislatore sia consapevolmente compiuta nella direzione di escludere l'applicabilità della valutazione d'impatto sui diritti fondamentali nelle ipotesi in cui il sistema di IA venga utilizzato secondo le modalità e ai fini di cui all'allegato III, punto 4, salvo l'assolvimento degli obblighi connessi alla DPIA non porti

incidentalmente – e, in ogni caso, guidato da una diversa finalità – il *deployer* a trattare aspetti che interessano anche la valutazione di impatto sui diritti fondamentali [223].

4. Sorveglianza e riesame umani.

L'ultimo strumento da prendere in considerazione ai fini della nostra analisi è il binomio sorveglianza-riesame umani dei sistemi IA e delle decisioni che questi possono assumere o supportare ad assumere. Seppur essenziali al presidio dell'antropocentrismo, il coinvolgimento degli attori collettivi nell' attuazione di tali strumenti è pressoché inesistente nel Regolamento IA, mentre appare continuo e costante nei sistemi automatizzati disciplinati dalla Direttiva sul lavoro mediante piattaforme digitali, fino a coprirne ogni fase dell'utilizzo.

Relativamente alla sorveglianza umana, tanto il Regolamento IA[224], quanto la proposta di Direttiva sul lavoro mediante piattaforme digitali garantiscono la supervisione da parte di persone fisiche dei sistemi di IA ad alto rischio e delle procedure automatizzate adottate.

Tuttavia, l'approccio adottato dai due atti legislativi appare parzialmente diverso.

Da una parte, entrambi dispongono che la sorveglianza debba essere affidata a persone fisiche dotate delle necessarie autorità, competenze e formazione e alle stesse riconoscono poteri tali da consentire loro, in un caso, di "individuare e affrontare anomalie, disfunzioni e prestazioni inattese" e "non usare il sistema di IA ad alto rischio o altrimenti di ignorar[n]e, annullar[n]e o ribaltar[n]e l'*output*", nell'altro di "non accogliere le decisioni automatizzate".

Dall'altra, se il Regolamento IA non sembra essere progettato in questa circostanza per momenti di coinvolgimento dei rappresentanti delle persone interessate, la proposta di Direttiva succitata introduce una "valutazione dell'impatto delle decisioni individuali prese o sostenute dai sistemi decisionali o di monitoraggio automatizzati", da svolgere con cadenza almeno biennale – e, dunque, costante e continua –, che vede la partecipazione anche dei rappresentanti dei lavoratori, i quali, in ogni caso, sono destinatari delle informazioni che vengono raccolte nell'ambito della suddetta valutazione.

Il Regolamento IA sembra discostarsi dalla proposta di Direttiva sul lavoro mediante piattaforme digitali anche rispetto alla configurazione della fase del riesame umano, risultando sprovvisto di una disposizione che consenta all'interessato di chiedere e ottenere un completo riesame della decisione adottata dal *deployer* sulla base di un *output* elaborato da un sistema di IA.

Un simile strumento, sulla scorta della descrizione fornita dall' nell'art. 11 della proposta

[223] V. contra ZAPPALÀ L., *Sistemi di IA ad alto rischio e ruolo del sindacato alla prova del* risk-based approach, in *Labour & Law Issues*, 2024, 1,10, I.66.
[224] Il riferimento è all'art. 14.

di Direttiva sul lavoro mediante piattaforme digitali, dovrebbe costituirsi di due fasi: la prima, finalizzata ad ottenere una spiegazione circa la decisione che è stata adottata dal sistema che si sta considerando; la seconda dovrebbe consentire all'interessato, e ai rappresentanti dell'interessato che agiscono per suo conto, di chiedere un riesame di tale decisione, in quanto ritiene che stia perpetrando la violazione di un suo diritto, ed eventualmente ottenere una rettifica della decisione stessa.

Tuttavia, l'art. 86 del Regolamento IA, pur riconoscendo alla persona interessata da una decisione del *deployer* basata sui sistemi IA potenzialmente in grado di incidere negativamente sulla sua salute, sulla sua sicurezza e sui diritti fondamentali "il diritto di ottenere dal *deployer* spiegazioni chiare e significative sul ruolo del sistema di IA nella procedura decisionale e sui principali elementi della decisione adottata", non fa seguire alcuna fase di revisione o rettifica della stessa e non prefigura alcuno spazio di agibilità per i rappresentanti dei soggetti interessati.

5. Conclusioni.

L'analisi condotta in queste pagine in merito alle soluzioni adottate dal Regolamento IA e dalle altre fonti che intervengono anche sui sistemi di IA dimostra un approccio non uniforme rispetto al ruolo degli attori collettivi e al loro coinvolgimento lungo la catena che vede utilizzati i sistemi di IA negli ambienti di lavoro, inevitabilmente, influenzato dalla diversa base giuridica delle fonti, che nel caso specifico del Regolamento IA non ha matrice giuslavoristica.

L'effetto è un "frettoloso" riferimento alle questioni dell'informazione e del coinvolgimento dei lavoratori nei casi di sistemi di IA ad alto rischio implementati nei luoghi di lavoro, compensata da una più elevata procedimentalizzazione delle informazioni che vengono scambiate ad un diverso livello, quello tra fornitore e *deployer*.

A ciò si aggiunga che, da una parte, la proposta di Direttiva sul lavoro mediante piattaforme digitali, una volta entrata in vigore, interverrà anche sui procedimenti che implementano la tecnica dell'IA, dall'altra, stante la sua portata settoriale, la gran parte delle situazioni lavorative non potranno contare su un apparato normativo sistematico. In tali casi, si dovrà ricorrere ad un'applicazione casistica delle disposizioni già esistenti, talvolta non espressive del più attuale spirito del legislatore europeo, orientato al maggior coinvolgimento degli attori collettivi nelle diverse fasi che scandiscono l'organizzazione e la gestione delle attività svolte dai lavoratori in contesti lavorativi sempre più digitalizzati.

L'obiettivo, finalizzato anche a garantire l'antropocentrismo nei sistemi di IA e

automatizzati, dovrebbe convergere verso un maggior coinvolgimento orizzontale e verticale dei lavoratori e dei loro rappresentanti in tali processi di trasformazione delle imprese per via dell'utilizzo dei sistemi di IA, realizzando quell'approccio di partenariato circolare continuo costruito dalle parti sociali europee nel 2020[225] per affrontare in maniera tempestiva la trasformazione digitale in chiave di ottimizzazione dei benefici che la stessa può comportare in "tempo reale".

La crescente de-umanizzazione delle relazioni lavorative non dovrebbe far perdere di vista la centralità dei lavoratori e dei diritti che devono essere loro garantiti. Per ribilanciare lo squilibrio determinato dall'intensificazione dei poteri datoriali per mezzo delle nuove tecnologie, il contributo delle parti sociali acquista un rilievo essenziale. È opportuno promuovere una dimensione dialogica, tipica dell'approccio europeo e poco garantita in questo Regolamento adottato dall'UE, orientata al raggiungimento di più livelli di democrazia all'interno dell'impresa.

A tal riguardo, nell'Accordo quadro delle parti sociali europee sulla digitalizzazione succitato l'IA e la garanzia del principio del controllo umano vengono considerate quali questioni da affrontare mediante l'applicazione di tale metodo di partenariato circolare e diversi aspetti che si ritrovano disciplinati nel Regolamento erano già stati presi in considerazione. Tra questi emerge la necessità di soffermarsi sulla trasparenza e sulla spiegabilità dei processi decisionali, che le parti sociali suggeriscono di modulare in relazione al contesto, alla gravità e alle conseguenze dell'utilizzo dei sistemi di IA.

Gli orientamenti delle parti sociali europee, dunque, sembrano voler evitare un'iper-informazione, che potrebbe costituire un ostacolo al raggiungimento di efficaci livelli di conoscenza dei sistemi IA, e dirigersi verso un'informazione "funzionale".

Tale considerazione mette in evidenza come in contesti lavorativi sempre più digitalizzati, innovativi e automatizzati anche i sindacati e i rappresentanti dei lavoratori dovrebbero maturare una maggiore predisposizione alla costruzione di un profilo "tecnico" per poter affrontare più efficacemente le sfide dell'IA, oltre a mostrare la necessità di un maggior ricorso all'affiancamento di questi ultimi da parte di soggetti esperti[226].

[225] Accordo Quadro delle parti sociali europee sulla digitalizzazione.
[226] V. anche CIUCCIOVINO S, *op. cit.*

INNOVAZIONE, PICCOLE E MEDIE IMPRESE E START−UP. PRIME OSSERVAZIONI IN MERITO AL REGOLAMENTO SULL'INTELLIGENZA ARTIFICIALE

Veronica Palladini
Dottoressa di ricerca in Lavoro Sviluppo e Innovazione, Università degli Studi di Modena e Reggio Emilia, Fondazione Marco Biagi

SOMMARIO: 1. Considerazioni preliminari: il quadro normativo europeo a sostegno dell'innovazione delle imprese di più piccole dimensioni. - 2. La disciplina prevista dal Regolamento sull'Intelligenza artificiale per le piccole e medie imprese e le *start-up*. - 3. Qualche considerazione conclusiva.

1. Considerazioni preliminari: il quadro normativo europeo a sostegno dell'innovazione delle imprese di più piccole dimensioni.

All'interno del Regolamento sull'intelligenza artificiale[227] il Legislatore europeo ha valutato opportuno dedicare un intero Capo, il VI, alle misure a sostegno dell'innovazione con l'obiettivo di incentivare il progresso, facilitare l'acquisizione di una maggior competitività dell'Unione europea sul mercato internazionale, anche al fine di superare la dipendenza economica dai Paesi al di là dell'Atlantico.

Tra le misure selezionate come necessarie per dar corso al proprio progetto, a fianco alla disciplina prevista per le cd. *sandbox* − oggi anche definite "spazi di sperimentazione normativa per l'IA"[228] − che assume un ruolo centrale nel processo di innovazione, si è posto l'accento su specifiche disposizioni a sostegno dei fornitori[229] e dei *deployer*[230] strutturati nella forma di piccole o medie imprese[231] e di *start-up*. Del resto, che *start-up* e PMI necessitino di misure a sostegno nonché – talvolta – di deroghe dall'applicazione dei vincoli più stringenti

* Relazione al Seminario "Lavoro, impresa e nuove tecnologie dopo l'AI Act" svoltosi il 14 maggio 2024 presso la Fondazione Biagi.

[227] D'ora in avanti anche solo "AI ACT" o "Regolamento".

[228] Secondo l'art. 3, par.1, n. 55 si definisce spazio di sperimentazione normativa per l'IA "un quadro controllato istituito da un'autorità competente che offre ai fornitori o potenziali fornitori di sistemi di IA la possibilità di sviluppare, addestrare, convalidare e provare, se del caso in condizioni reali, un sistema di IA innovativo, conformemente a un piano dello spazio di sperimentazione per un periodo di tempo limitato sotto supervisione regolamentare";

[229] Con "fornitore" il Regolamento sull'intelligenza artificiale allude ad una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che sviluppa un sistema di IA o un modello di IA per finalità generali o che fa sviluppare un sistema di IA o un modello di IA per finalità generali e immette tale sistema o modello sul mercato o mette in servizio il sistema di IA con il proprio nome o marchio, a titolo oneroso o gratuito (art. 3, par.1, n. 3 AI ACT).

[230] Fin da subito è bene intendere che il *deployer* è quella persona fisica o giuridica, autorità pubblica, agenzia o altro organismo che utilizza un sistema di IA sotto la propria autorità, nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività professionale (art. 3, par.1, n. 4 AI ACT).

[231] Nel prosieguo anche indicate con l'acronimo "PMI".

non è una considerazione nuova in capo al Legislatore eurounitario che con la nuova stagione giuridico-normativa a cui ha dato il via tramite l'adozione di numerosi atti, per lo più di natura regolamentare, ha sempre mantenuto un atteggiamento di favore verso quelle realtà imprenditoriali che − per quanto prese singolarmente non producano effetti impattanti nel mercato europeo − in ragione della loro numerosità e capillarità assumono una notevole importanza nel tessuto economico europeo. Potremmo addirittura attribuire a tale opzione il *nomen* di "approccio europeo"[232], espressione con cui possiamo alludere a quell'azione tipica delle Istituzioni europee che nell'attuare un equilibrio tra protezione dei soggetti e salvaguardia dei produttori, attraverso un approccio basato sul rischio, tiene conto in particolare delle piccole e medie imprese impiegate nel settore di riferimento con l'obiettivo di assicurare la ragionevolezza dell'intervento normativo.

Di questa riflessione ne è certamente un esempio il *Regolamento sulla Governance dei dati*[233], che al considerando 2 nell'affermare che "L'economia dei dati deve essere creata in modo da consentire alle imprese, in particolare alle microimprese e alle piccole e medie imprese (PMI) […] e alle *start-up*, di prosperare, garantendo neutralità dell'accesso ai dati e portabilità e interoperabilità dei dati, ed evitando effetti di dipendenza ("lock-in")" traduce con estrema franchezza la necessità, oramai non più rinviabile, di controbilanciare la spregiudicatezza dei *gatekeeper,* in favore della proliferazione di un sistema maggiormente concorrenziale anche aperto alle più piccole imprese[234].

[232] Per una riflessione, seppur sotto altra prospettiva, sull' "approccio europeo" si veda CHIAPPINI D., *Intelligenza Artificiale e responsabilità civile: nuovi orizzonti di regolamentazione alla luce dell'Artificial Intelligence Act dell'Unione europea,* in *Rivista italiana di informatica e diritto,* Firenze, 2, 2022, 98, *https://www.rivistaitalianadiinformaticaediritto.it/index.php/RIID/article/view/121*.

[233] Regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio del 30 maggio 2022 relativo alla governance europea dei dati e che modifica il Regolamento (UE) 2018/1724 (Regolamento sulla governance dei dati), *https://eur-lex.europa.eu/legal-content/it/txt/?uri=celex%3a32022r0868*.
A favore delle PMI, all'interno del *Regolamento sulla Governance dei dati*, non possono essere tralasciate le previsioni che consentono agli enti pubblici di imporre tariffe ridotte o nulle, compatibilmente con la normativa sugli aiuti di Stato, nei confronti di PMI e *start-up* per incentivare il riutilizzo delle categorie di dati disciplinate dallo stesso Regolamento (art. 6); nonché quelle che consentono che i canali di informazione rivolti a PMI e *start-up* possano essere distinti dagli altri e maggiormente semplificati oltre che ben documentati (art. 8); ulteriormente, quelle che prevedono tariffe ridotte nulle per la notifica da parte dei fornitori di servizi di intermediazione dei dati all'autorità competente per i servizi di intermediazione dei dati (art. 11).

[234] Meritano di essere ricordate anche le osservazioni di SCAGLIARINI S., *Identità digitale e tutela della privacy*, Intervento presentato al convegno *Il diritto costituzionale e le sfide dell'innovazione tecnologica*, tenutosi a Genova il 18-19 giugno 2021, in *Quaderni del Gruppo di Pisa*, *gruppodipisa.it*, 2022, che a pagina 369 afferma *"la posizione dominante di queste imprese appare via via crescente e in corso di consolidamento, grazie a frequenti operazioni di incorporazione di nuove realtà imprenditoriali emergenti in forma di start-up, che ben rientrano nel novero delle concentrazioni, pure oggetto di disciplina antitrust"*. Sul punto *ex multis* anche. BETZU M., *I poteri privati nella società digitale: oligopoli e antitrust*, in *Diritto pubblico*, Il Mulino, Bologna, n. 3, 2021, 739-760; IANNOTTI DELLA VALLE A., *Le regole di internet tra poteri pubblici e privati, tutela dei diritti e ruolo dell'antitrust in una prospettiva costituzionale*, Editoriale scientifica, Napoli, 2023.

Sulla medesima scia, ma con un diverso approccio si pone il *Regolamento europeo sui mercati digitali*[235](anche solo "DMA") che ponendosi proprio l'obiettivo di ripristinare un mercato concorrenziale, al considerando 24, chiarisce che nel valutare il ruolo di *gatekeeper* delle imprese che forniscono servizi di piattaforma di base che non raggiungono tutte le soglie quantitative alla luce dei requisiti oggettivi[236] stabiliti dal Regolamento, occorre mantenere un approccio maggiormente attento nel caso in cui a fornire tali servizi sia una PMI o una microimpresa. Considerato infatti che il DMA è destinato principalmente a grandi imprese dotate di considerevole potere economico, nel caso in cui siano coinvolte imprese di dimensioni medie o piccole, la valutazione dovrebbe dunque prendere attentamente in considerazione l'eventualità che tale impresa possa compromettere in modo sostanziale la contendibilità del mercato di riferimento.

Il Legislatore eurounitario rivolge poi una particolare attenzione alle PMI pure all'interno del *Regolamento europeo sui servizi digitali*[237] (anche conosciuto come "DSA") − la normativa che stabilisce regole e obblighi alle quali i prestatori di servizi intermediari e i fornitori di piattaforme online nell'Unione Europea sono tenuti a conformarsi al fine di garantire la sicurezza e la trasparenza nel contesto digitale − escludendo espressamente dall'applicazione delle sezioni cruciali del Regolamento (Capo III Sezioni 3[238], 4[239] e inevitabilmente 5[240]) le microimprese e le piccole imprese salvo che non siano piattaforme di grandi dimensioni.

Ora, tale riflessione non poteva che confluire anche nel più recente e discusso testo di legge elaborato dall'Europa, per quanto la decisione di introdurre disposizioni di maggior

---

235 Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (Regolamento sui mercati digitali), *https://eur-lex.europa.eu/legal-content/it/txt/?uri=celex%3a32022r1925*.

236 L'art. 3 del DMA afferma che un'impresa è designata come gatekeeper se: a) ha un impatto significativo sul mercato interno ovvero se raggiunge un fatturato annuo nell'Unione pari o superiore a 7,5 miliardi di EUR in ciascuno degli ultimi tre esercizi finanziari, o se la sua capitalizzazione di mercato media o il suo valore equo di mercato equivalente era quanto meno pari a 75 miliardi di EUR nell'ultimo esercizio finanziario, e se essa fornisce lo stesso servizio di piattaforma di base in almeno tre Stati membri; b) fornisce un servizio di piattaforma di base che costituisce un punto di accesso (gateway) importante affinché gli utenti commerciali raggiungano gli utenti finali ovvero se fornisce un servizio di piattaforma di base che, nell'ultimo esercizio finanziario, annovera almeno 45 milioni di utenti finali attivi su base mensile, stabiliti o situati nell'Unione, e almeno 10 000utenti commerciali attivi su base annua stabiliti nell'Unione, identificati e calcolati conformemente alla metodologia e agli indicatori di cui all'allegato; e c) detiene una posizione consolidata e duratura, nell'ambito delle proprie attività, o è prevedibile che acquisisca siffatta posizione nel prossimo futuro ovvero se le soglie di cui alla lettera b) sono state raggiunte in ciascuno degli ultimi tre esercizi finanziari.

237 Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la Direttiva 2000/31/CE (Regolamento sui servizi digitali), *https://eur-lex.europa.eu/legal-content/it/txt/?uri=celex%3a32022r2065*.

238 Nella sezione III del capo III sono inserite le disposizioni aggiuntive applicabili ai fornitori di piattaforme online.

239 Che prevede le disposizioni aggiuntive applicabili ai fornitori di piattaforme online che consentono ai consumatori di concludere contratti a distanza con gli operatori commerciali.

240 La sezione 5 del capo III del DSA disciplina gli obblighi supplementari a carico dei fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi per la gestione dei rischi sistemici.

favore per incentivare l'impiego di sistemi di intelligenza artificiale anche nelle imprese meno strutturate non sia nata unitamente alla prima formulazione del testo legislativo.

Se, infatti, come abbiamo visto la scelta di prevedere regimi talora incentivanti o alle volte derogatori per le PMI non pare nuova per il Legislatore europeo, in realtà non si può tralasciare di ricordare che la necessità di recepire analoghe considerazioni anche all'interno del AI ACT sia frutto di innesti normativi affiorati dopo la prima stesura del testo. L'art 55 della proposta originaria prevedeva, invero, in capo agli Stati membri soltanto il rispetto dei seguenti obblighi: l'onere di adottare misure volte a riconoscere ai fornitori di piccole dimensioni e alle *start-up* un accesso prioritario agli spazi di sperimentazione normativa per l'IA; l'obbligo di organizzare specifiche attività di sensibilizzazione sull'applicazione del Regolamento; la previsione di istituire un canale dedicato per la comunicazione con i fornitori di piccole dimensioni e, infine, di stabilire tariffe per la valutazione della conformità che tenessero conto degli interessi e delle esigenze specifici dei fornitori di piccole dimensioni, riducendo tali tariffe proporzionalmente alle loro dimensioni e alle dimensioni del loro mercato. Così facendo, il Legislatore europeo avrebbe lasciato agli Stati membri il compito di adottare misure di sostegno per le piccole e medie imprese, operazione che, a parere di molti, generava il rischio che le PMI e le *start-up* non partecipassero neppure al processo di innovazione, rischio che la previsione secondo cui nel fissare le tariffe per la valutazione della conformità si sarebbe dovuto tenere conto degli interessi e delle esigenze specifici dei fornitori di piccole dimensioni non valeva ad affievolire.

Del resto, la necessità di introdurre norme a sostegno delle PMI, era un'esigenza avvertita da più parti e che poggia le sue basi in studi che oggi, con la rapidità dell'evoluzione a cui siamo sottoposti, potremmo già definire risalenti. Ne sono un esempio le considerazioni contenute nello *Study on the relevance and impact of artificial intelligence for company law and corporate governance, 2021*[241]*,* in cui si evidenzia che *"*the level of AI use in CL&CG[242]in Europe will likely be subject only to a limited increase, at least in the short term. Existing differences in sectors and company-sizes are also likely to remain in place, with large companies in certain industries (i.e. the financial sector) more prone to adopting AI solutions than SMEs"[243].

Che le grandi imprese utilizzino l'intelligenza artificiale più delle piccole e medie imprese è un dato di fatto: dall'analisi Eurostat dedicata all'*Utilizzo dell'intelligenza artificiale nelle imprese*[244]

[241] COMMISSIONE EUROPEA, DIREZIONE GENERALE DELLA GIUSTIZIA E DEI CONSUMATORI, *Studio sulla rilevanza e l'impatto dell'intelligenza artificiale per il diritto societario e la governance aziendale* – Relazione finale, Ufficio delle pubblicazioni, 2021, *https://data.europa.eu/doi/10.2838/790784*.
[242] Con l'abbreviazione "*CL&CG"* all'interno dello studio si fa riferimento alle *company law and corporate governance.*
[243] Acronimo che allude alle *small and medium-sized enterprises.*
[244] Lo studio che ha per oggetto dati estratti a dicembre 2023, si è arrestato all'analisi delle imprese con più di 10 dipendenti, *https://ec.europa.eu/eurostat/statistics-*

del 2021, se il 28% delle grandi imprese hanno utilizzato l'IA, soltanto il 13% delle medie imprese e il 6% delle piccole imprese, ne ha fatto uso. Differenza che ben potrebbe trovare una spiegazione nella complessità dell'implementazione delle tecnologie di intelligenza artificiale – le imprese con maggiori economie di scala possono trarre maggiori benefici dall'intelligenza artificiale – nonché nei costi di investimento che le tecnologie di IA richiedono per la loro applicazione. A ciò si somma il fatto che il modello di gestione del rischio[245] adottato dal Regolamento sull'intelligenza artificiale, comporta oneri amministrativi rilevanti il cui costo, come rileva attenta dottrina[246], graverà sulle imprese. In capo ai fornitori di sistemi di intelligenza artificiale ad alto rischio sono, infatti, imposti dallo stesso Regolamento significativi oneri tra i quali: l'istituzione di un sistema di gestione della qualità che garantisca la conformità al Regolamento[247]; la sottoposizione del sistema di gestione della qualità alla procedura di valutazione di conformità per i soggetti obbligati[248]; la redazione della documentazione tecnica del sistema ad alto rischio[249]; l'apposizione della marcatura CE[250]; la conservazione dei *log* generati automaticamente[251]; la registrazione del sistema nella banca dati UE[252] *etc.*

---

explained/index.php?title=Use_of_artificial_intelligence_in_enterprises#Enterprises_using_artificial_i

[245] Sul modello di gestione del rischio adottato dal Regolamento sull'intelligenza artificiale, *ex plurimus*, si ricordano i contributi di FINOCCHIARO G., *La regolazione dell'intelligenza artificiale*, in *Riv. Trimest. Dirit. Pubblico*, n. 4, 2022, Giuffrè, Milano, 1093 ss; MARCHETTI B., CASONATO C., *Prime osservazioni sulla proposta di Regolamento dell'Unione europea in materia di intelligenza artificiale*, in *BioLaw Journal*, n. 3 2021, 415-437 in *https://teseo.unitn.it/biolaw/article/view/1793*; FINOCCHIARO, G., *La proposta di Regolamento sull'intelligenza artificiale: il modello europeo basato sulla gestione del rischio*, in *La via europea per l'Intelligenza Artificiale*, Intervento presentato al convegno Progetto Dottorale di Alta Formazione in Scienze Giuridiche tenutosi a Venezia nel 25-26 novembre 2021, 2022, 215-237; SIMONCINI A., *Verso la regolamentazione della Intelligenza Artificiale. Dimensioni e governo* in *BioLaw Journal*, n. 2, 2021, 411-417, *https://teseo.unitn.it/biolaw/article/view/1672*; CONTISSA G., GALLI F., GODANO F., SARTOR G., *Il regolamento europeo sull'intelligenza artificiale*, in *Rivista semestrale on-line: www. i-lex. It*, 2021; SARTOR G., *L'intelligenza artificiale e il diritto*, 2022, Giappichelli, Torino, 93 ss; DI CIOMMO, I. P., *La prospettiva del controllo nell'era dell'Intelligenza Artificiale. Alcune osservazioni sul modello Human In The Loop,* in *federalismi.it*, n. 9, 2023,71 ss.

[246] FINOCCHIARO G., *La regolazione dell'intelligenza artificiale*, cit., 1096-1097.

[247] Considerata la difficoltà di garantire un'elevata qualità di prodotti ancora per lo più sconosciuti, la conformità ai requisiti del Regolamento, nell'ottica dell'AI ACT, viene assicurata attraverso l'adozione di un sistema di gestione della qualità: nell'era della tecnica la garanzia di qualità del prodotto diviene garanzia di conformità normativa.
Sul tema ricordiamo il contributo di ROMANÒ L., *La responsabilità penale al tempo di ChatGPT* in *Sistema penale*, 2023, 19-20, *https://www.sistemapenale.it/it/articolo/romano-la-responsabilita-penale-al-tempo-di-chatgpt-prospettive-de-iure-condendo-in-tema-di-gestione-del-rischio-da-intelligenza-artificiale-generativa*, che allude proprio ad un approccio regolativo proattivo.

[248] Si veda in proposito la sezione V del capo III del Regolamento, specificamente dedicata a *Norme, valutazione della conformità, certificati, registrazione* che, anche rinviando agli Allegati VI e VII, delinea un articolato sistema di valutazione della conformità dei sistemi ad alto rischio.

[249] Per un approfondimento si veda l'art. 11 AI ACT integrato dall'Allegato IV del Regolamento.

[250] L'obbligo di marcatura è disciplinato dall'art. 48 che a sua volta rinvia ai principi generali di cui all'articolo 30 del regolamento (CE) n. 765/2008.

[251] Come descritti rispettivamente dagli artt. 12 (inserito tra i requisiti che devono possedere i sistemi di intelligenza artificiale ad alto rischio) e 19 del Regolamento (nella sezione specificamente dedicata agli obblighi lungo la catena di valore dell'IA).

[252] Cfr. articolo 49 del Regolamento che prevede che prima di immettere sul mercato o mettere in servizio un sistema di IA ad alto rischio, salvo deroghe ed eccezioni, il fornitore o, ove applicabile, il rappresentante

Stringenti ulteriori requisiti sono poi riconosciuti in capo all'intera filiera o, come definita dal Regolamento stesso, lungo tutta la "catena del valore dell'IA" non solo rispetto alla progettazione e produzione ma anche alla distribuzione, all'importazione e all'utilizzo dei sistemi di intelligenza artificiale attribuendo a ciascun soggetto partecipante obblighi e relative responsabilità[253].

Orbene, come rilevava autorevole dottrina,[254] il modello di gestione del rischio scelto dall'UE nel Regolamento sull'intelligenza artificiale comporta oneri anche economici nei confronti di fornitori e *deployer* di non poco conto e la scelta di gravare le imprese indistintamente − ovvero a prescindere dalle loro dimensioni − di tali fardelli non poteva che rappresentare un limite alla partecipazione al mercato dei più modesti operatori economici.

Per tale ragione, in un'ottica di maggior ragionevolezza, anche a seguito di consultazione pubblica, Parlamento e Consiglio hanno inteso rivedere il testo originario e a seguito di lunghi ed intesi negoziati hanno raggiunto un Accordo sul Testo di Regolamento volto ad includere misure a sostegno dell'innovazione e di piccole e medie imprese, affinché le PMI – riferisce l'Europarlamento – possano, riprendendo le considerazioni mosse poc'anzi, "sviluppare soluzioni di AI senza pressioni indebite da parte dei giganti dell'industria che controllano la catena del valore".

2. La disciplina prevista dal Regolamento sull'Intelligenza artificiale per le piccole e medie imprese[255] e le *start-up.*

autorizzato si registra e registra il suo sistema nella banca dati dell'UE di cui all'articolo 71 del Regolamento.

[253] Specificamente dedicati agli obblighi dei deployer dei sistemi di IA ad alto rischio e di altre parti, sono gli articoli 23-27 del Regolamento.

[254] Esprime magistralmente tale preoccupazione Finocchiaro che nel commentare il testo della proposta afferma che "questo errore, cioè adottare la medesima soluzione per soggetti e ambiti assai diversi fra loro, è stato già commesso in altri settori dell'ordinamento, per esempio con riguardo proprio alla disciplina in materia di trattamento dei dati personali, che poi, infatti, in tempi più recenti, è stata ripensata con il principio dell'accountability per consentire di modulare le misure da adottare in ragione delle caratteristiche proprie del caso specifico. Gli obblighi dettati dal legislatore europeo produrranno naturalmente effetti differenti a seconda dei soggetti nei confronti dei quali si rivolgono. Le società di grandi dimensioni presumibilmente non avranno problemi a gestire oneri di documentazione, certificazione, marcatura e quant'altro. Le piccole imprese, e in particolare le start-up, invece, vedranno oneri economici molto pesanti e rilevanti a seguito degli obblighi previsti dal legislatore europeo" FINOCCHIARO G., *La regolazione dell'intelligenza artificiale*, cit., 1096-1097.

[255] Ai sensi del Regolamento sull'intelligenza artificiale si definiscono PMI le imprese che occupano meno di 250 persone e il cui fatturato annuo non supera i 50 milioni di EUR oppure il cui totale di bilancio annuo non supera i 43 milioni di EUR (Raccomandazione 2003/361/CE). Più nel dettaglio l'art. 2 Raccomandazione 2003/361/CE, definisce: a) medie le imprese che occupano meno di 250 persone, il cui fatturato annuo non supera i 50 milioni di EUR oppure il cui totale di bilancio annuo non supera i 43 milioni di EUR; b) piccole le imprese che occupano meno di 50 persone e realizzano un fatturato annuo o un totale di bilancio annuo non superiori a 10 milioni di EUR; c) micro le imprese che occupano meno di 10 persone e realizzano un fatturato annuo oppure un totale di bilancio annuo non superiori a 2 milioni di EUR.

Allo scopo di creare un quadro giuridico più favorevole all'innovazione, a seguito dell'accordo di Parlamento e Consiglio, come chiarisce quest'ultimo[256], le disposizioni relative alle misure a sostegno dell'innovazione sono state sostanzialmente modificate rispetto alla proposta della Commissione. A conferma, il considerando 8 dell'AI ACT che nella sua ultima formulazione, proprio al fine di rendere esplicita la necessità che il quadro giuridico dell'Unione preveda norme chiare e solide anche al fine di sostenere nuove soluzioni innovative e consentire un ecosistema europeo in linea con i valori dell'Unione che sblocchino il potenziale della trasformazione digitale, mette in luce la necessità di stabilire misure a sostegno delle piccole e medie imprese[257]. Al fine di non porre sulle spalle di questi attori del mercato, vera ossatura dell'apparato produttivo europeo, un peso eccessivo dunque il Legislatore eurounitario ha ritenuto di ridurre al minimo, laddove possibile senza pregiudicare la tutela dei diritti fondamentali dei cittadini europei, alcuni dei più impattanti oneri introdotti dal Regolamento[258].

Ne è un esempio l'introduzione di una specifica previsione all'interno dell'art. 11 AI ACT in cui si chiarisce che la documentazione tecnica[259] – finalizzata a dimostrare che il sistema di IA ad alto rischio è conforme ai requisiti richiesti dal Regolamento – può essere redatta in modalità semplificate per le PMI e le *start-up* anche tramite, aspetto di maggior rilievo, un modulo di documentazione tecnica e semplificata redatto a tal scopo dalla Commissione[260].

Ora, il trasferimento in capo alla Commissione dell'onere di predisporre un modulo specificamente adattato alle esigenze delle piccole e medie imprese risulta, a nostro parere, una soluzione di grande favore per le più piccole realtà imprenditoriali considerato che in tal modo esse saranno esonerate dall'individuazione delle modalità semplificate, con il rischio di

---

256 CONSIGLIO DELL'UNIONE EUROPEA, COMUNICATO STAMPA 9 DICEMBRE 2023*, Regolamento sull''intelligenza artificiale: il Consiglio e il Parlamento raggiungono un accordo sulle prime regole per l'IA al mondo*. Il comunicato stampa è stato aggiornato il 2 febbraio 2024, *https://www.consilium.europa.eu/it/press/press-releases/2023/12/09/artificial-intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai.*

257 Il considerando 8 recita "(8) Si rende pertanto necessario un quadro giuridico dell'Unione che istituisca regole armonizzate in materia di IA per promuovere lo sviluppo, l'uso e l'adozione dell'IA nel mercato interno […]. Tali norme dovrebbero […] sostenere nuove soluzioni innovative e consentire un ecosistema europeo di attori pubblici e privati che creino sistemi di IA in linea con i valori dell'Unione e sblocchino il potenziale della trasformazione digitale in tutte le regioni dell'Unione. Stabilendo tali regole nonché le
misure a sostegno dell'innovazione, con particolare attenzione alle piccole e medie imprese (PMI), comprese le start-up […]". Il corsivo indica i più recenti interventi sul testo originale.

258 BELOTTI P., *I codici di condotta di cui alla Proposta di Regolamento UE sull'Intelligenza Artificiale: Ipotesi per un'applicazione dello Human Rights-Based Approach,* in *i-lex – Rivista di Scienze Giuridiche, Scienze Cognitive e Intelligenza Artificiale,* vol 15, n. 2, Bologna, 2022, 55, *https://i-lex.unibo.it/article/view/17109/16043*.

259 La documentazione tecnica richiesta è descritta nell'allegato IV.

260 L'art. 11 AI ACT prevede testualmente che "Le PMI, comprese le start-up, possono fornire in modo semplificato gli elementi della documentazione tecnica specificati nell'allegato IV. A tal fine la Commissione definisce un modulo di documentazione tecnica semplificata che risponda alle esigenze delle piccole imprese e delle microimprese. Qualora una PMI, compresa una start-up, decida di fornire in modo semplificato le informazioni richieste nell'allegato IV, utilizza il modulo di cui al presente paragrafo. Gli organismi notificati accettano il modulo ai fini della valutazione della conformità".

affidarsi a valutazioni contestabili, e dovranno "semplicemente" adeguarsi a requisiti definiti dall' "alto", sollevandole così dalla necessità di selezionare le modalità semplificate di adeguamento, che si tradurrebbe altrimenti in inevitabili ulteriori esborsi da devolvere a società di consulenza e professionisti a cui rivolgersi per farsi supportare nell'adeguamento.

Un ruolo centrale nel garantire la partecipazione all'innovazione delle PMI è poi l'istituzione di un forum consultivo[261] per i portatori di interessi, tra i quali compaiono anche le PMI e le *start-up* al fine di fornire competenze tecniche al Comitato per l'IA[262]. In questo modo orientandosi sempre più verso una strategia preventiva che mira a coinvolgere direttamente gli operatori nella determinazione delle regole da rispettare nello sviluppo e nell'utilizzo di sistemi intelligenti[263] ovvero, come chiarisce l'art. 62, par. 1, let. d), nel processo di sviluppo della normazione.

Anche in questo caso la soluzione pensata dal Legislatore eurounitario non può che ritenersi apprezzabile, tanto più se si considera che ai sensi dell'art. 40 AI ACT, i sistemi di IA ad alto rischio si presumono conformi al Regolamento se sono conformi alle norme armonizzate conformemente al Regolamento (UE) n. 1025/2012 nella misura in cui esse contemplino i requisiti di cui alla sezione 2 del Capo III del Regolamento. Se si considera, dunque, che tra i requisiti di Conformità dell'AI ACT vi è il rispetto delle norme armonizzate (a condizione che esse, come detto, contemplino il rispetto degli artt. 8-15 del Regolamento) risulta particolarmente apprezzabile che il Legislatore eurounitario − ribadendo quanto già affermato dal considerando 2 del Regolamento (UE) n. 1025/2012[264] − coinvolga i più piccoli attori del mercato nei processi di normazione, e dunque ai sensi dell'AI ACT di adeguamento alla conformità, sì da contribuire, per il tramite di detta partecipazione, anche a promuovere la competitività delle imprese.

Non potevano poi mancare interventi specificamente dedicati a favorire la partecipazione delle PMI agli spazi di sperimentazione normativa − nati al fine di creare un ambiente controllato per lo sviluppo, le prove e la convalida di sistemi di IA innovativi – che si

[261] Proprio in un'ottica di piena partecipazione, l'art. 67 AI ACT chiarisce che la composizione del forum consultivo vuole essere dimostrativa di una equilibrata selezione equilibrata di portatori di interessi commerciali e non commerciali e, all'interno della categoria degli interessi commerciali, per quanto riguarda le PMI e le altre imprese.

[262] Gli artt. 65 e 66 definiscono il Comitato europeo per l'intelligenza artificiale, anche solo "Comitato", come quell'organo composto di un rappresentante per Stato membro ai cui lavori partecipano anche il Garante europeo della protezione dei dati e l'ufficio per l'IA come osservatori, che fornisce consulenza e assistenza alla Commissione e agli Stati membri al fine di agevolare l'applicazione coerente ed efficace del Regolamento.

[263] ROMANÒ L., *La responsabilità penale al tempo di ChatGPT*, cit, 19-20.

[264] Il quale afferma che "Conformemente con i principi fondatori, è importante che tutte le pertinenti parti interessate, incluse le autorità pubbliche e le piccole e medie imprese (PMI), siano adeguatamente coinvolte nel processo di normazione nazionale ed europeo. Gli organismi di normazione nazionali dovrebbero altresì incoraggiare e facilitare la partecipazione dei soggetti interessati".

traducono della previsione di un elenco di azioni che dovranno essere intraprese per sostenere gli operatori più piccoli e nell'introduzione di alcune deroghe limitate e chiaramente specificate. Il Regolamento richiede perciò agli Stati membri di istituire tali spazi di sperimentazione normativa e meccanismi di prova in condizioni reali (le cd. *sandbox*) e renderli accessibili sicché le PMI e *start-up* possano in condizioni di privilegio − anche sotto il profilo degli oneri amministrativi − sviluppare sistemi di IA innovativi e addestrarli prima di immetterli sul mercato.

Di più, a dimostrazione del fatto che i principali destinatari di tali spazi di sperimentazione sono le PMI e le *start-up*, l'art. 62 par. 1 lett. a), chiarisce che a tali imprese, naturalmente nella misura in cui soddisfano le condizioni di ammissibilità e i criteri di selezione, deve essere garantito un accesso prioritario agli spazi di sperimentazione normativa per l'IA e che, soprattutto, ne sia garantito un accesso gratuito[265].

Affinché, tuttavia, le PMI possano effettivamente partecipare a tali spazi, nell'ottica dell'AI ACT occorre rimuovere gli ostacoli all'ingresso nonché (in concreto): dissipare le incertezze giuridiche, anche tramite l'utilizzo di canali dedicati per la comunicazione al fine di fornire consulenza in particolate per quanto riguarda la partecipazione agli spazi di sperimentazione normativa; organizzare specifiche attività di sensibilizzazione e formazione sull'applicazione del Regolamento adattandole alle esigenze delle PMI e delle *start-up*[266]. E per facilitare tale processo, ancora una volta la Commissione − tramite l'ente con cui opera ovvero l'Ufficio per l'IA[267] − viene investita del compito di fornire modelli standardizzati per facilitare l'adeguamento degli operatori al Regolamento (art. 62 par. 3, let. a) AI ACT).

Il Legislatore europeo è poi intervenuto pure sugli oneri amministrativi, avvertendo la necessità − per i soggetti tenuti a sottoporsi a valutazione di conformità − di stabilire tariffe che tengano conto degli interessi e delle esigenze specifici delle PMI e delle *start-up*, ovvero riducendo tali tariffe nel seguente modo: a) in misura proporzionata alle loro dimensioni; b) in misura proporzionata alle dimensioni del loro mercato; ma anche, c) in misura proporzionata ad altri indicatori pertinenti (art. 62 par. 2 AI ACT)[268]. Ora non possiamo

[265] La disposizione prevede anche che in via di eccezione le autorità nazionali competenti possano introdurre costi straordinari purché equi e proporzionati (art. 58 par. 2 lett. d) AI ACT).
[266] Cfr, considerando 138, artt. 62 par. 11, lett. b), c), art. 70 AI ACT.
[267] L' art. 3, n. 47 definisce l'Ufficio per l'IA, la funzione della Commissione volta a contribuire all'attuazione, al monitoraggio e alla supervisione dei sistemi di IA e della governance dell'IA svolta dall'ufficio europeo per l'intelligenza artificiale istituito con decisione della Commissione del 24.1.2024.
[268] Sul punto, il considerando 143 chiarisce che la Commissione dovrebbe valutare periodicamente i costi di certificazione e di conformità per le PMI, comprese le *start-up*, attraverso consultazioni trasparenti con i *deployer* e dovrebbe collaborare con gli Stati membri per ridurre tali costi, come ad esempio, i costi relativi alle spese di traduzione connesse alla documentazione obbligatoria e alla comunicazione con le autorità che possono essere significativi per i fornitori e gli altri operatori, in particolare quelli di dimensioni ridotte.

omettere di rilevare, con spirito critico, che per quanto tale previsione possa tradurre uno spirito di ragionevolezza certamente apprezzabile essa presti il fianco alle più disparate interpretazioni e a non poche incertezze, lasciando in capo agli organismi notificati[269], investiti di tale compito, l'individuazione di quali possano essere "gli altri indicatori pertinenti" con ampio margine di discrezionalità nell'individuazione delle circostanze che possono determinare l'applicazione di tariffe più basse. Infine, ma non certo per ordine di importanza, l'AI ACT ha ritenuto anche di prevedere massimali più proporzionati per le sanzioni amministrative pecuniarie per le PMI e le *start-up* in caso di violazione delle disposizioni del regolamento sull'IA. Sul punto l'art. 99 AI ACT chiarisce che nello stabilire le sanzioni − anche non pecuniarie −, gli Stati membri tengono conto degli interessi delle PMI e delle *start-up*, e della loro sostenibilità economica. In questo caso, contrariamente a quanto fatto in materia di oneri di conformità, riteniamo apprezzabile l'ampio margine di libertà affidato agli Stati membri, se si considera, come stabilisce l'art. 99 par. 9 AI ACT, da un lato che le sanzioni pecuniarie possono essere inflitte dai tribunali nazionali competenti o da altri organismi (pubblici) che quindi soddisfano requisiti di terzietà ed imparzialità; dall'altro, che ben può prevedersi un adeguamento dell'entità delle sanzioni che tenga conto anche dei limiti di fatturato tipici di questo genere di imprese.

3. Qualche considerazione conclusiva.

In conclusione, ci pare di poter affermare che il Legislatore europeo abbia inteso riconoscere alle piccole e medie imprese e alle *start-up* un vero ruolo di motore dell'innovazione.

Parlamento e Consiglio, ben consapevoli della spinta propulsiva insita in questi attori del mercato hanno voluto renderli destinatari − nella più recente formulazione del Testo legislativo ad oggi a disposizione − di diverse e specifiche previsioni intese a garantire loro un ruolo da protagonisti nell'economia *data driven*.

E del resto, che oramai in tutti i settori economici si faccia impiego di tecnologie basate sull'intelligenza artificiale e che allo stesso modo che essa sia impiegata in tutte le professioni (come dimostra la Corte di cassazione che per la prima volta, a nostra conoscenza, in una sua

[269] Gli organismi notificati secondo l'art. 33 AI ACT sono enti con personalità giuridica, indipendenti dal fornitore di un sistema di IA ad alto rischio che non intervengono direttamente nella progettazione, nello sviluppo, nella commercializzazione o nell'utilizzo di sistemi di IA ad alto rischio, né rappresentano i soggetti impegnati in tali attività. Gli organismi notificati, inoltre, non intraprendono alcuna attività che possa essere in conflitto con la loro indipendenza di giudizio o la loro integrità e mantengono la riservatezza delle informazioni di cui vengono in possesso nello svolgimento delle attività di valutazione della conformità. Sono, infine, responsabili per le loro attività di valutazione della conformità e a tal fine, sottoscrivono un'assicurazione di responsabilità.

recentissima pronuncia si occupa dell'uso di ChatGPT[270]) è un dato di fatto rispetto al quale anche le imprese di minori dimensioni per mantenersi al passo coi tempi devono far conto.

La scelta di rendere partecipi, con un ruolo non marginale, le PMI rispetto a quell'incessante progresso determinato dalla rivoluzione digitale in atto, non deriva solo dalla necessità di conservare in capo alle stesse il ruolo trainante che hanno sempre avuto, ma anche dall'esigenza di garantire lo sviluppo di imprese al passo con la modernità e dunque competitive, capaci di controbilanciare il potere delle *Big tech*, obiettivo che si pone in *continuum*, come già evidenziato, con le scelte già operate tramite l'introduzione del DMA e del DSA.

I poteri delle grandi società, che difficilmente possono essere ridimensionati dai Governi nazionali, potrebbero essere più efficacemente compensati dalla forza delle eccellenze imprenditoriali nazionali ed europee ancorché, singolarmente considerate, di piccole e medie dimensioni, ma che riunite possono – a nostro avviso più efficacemente dei governanti− contribuire al ripristino di un mercato maggiormente equilibrato.

Ora, rappresentano una chiara estrinsecazione di tali considerazioni l'incentivo anche economico alla partecipazione delle PMI agli spazi di sperimentazione normativa, ma anche il contributo che esse sono spronate ad apportare tramite la partecipazione al forum consultivo, nonché la spinta a contribuire allo stesso processo di normazione.

Inoltre, sotto altro punto di vista, le Istituzioni europee, con un approccio particolarmente apprezzabile, hanno previsto alcune semplificazioni nei confronti delle PMI e delle *start-up* riconoscendo loro l'opportunità di adeguarsi agli oneri documentali in maniera semplificata ovvero attraverso moduli a tal fine predisposti dalla Commissione. Ancora, in un'ottica di eguaglianza sostanziale, pare ragionevole ed equilibrata la scelta di introdurre la possibilità di adeguare il trattamento sanzionatorio alla sostenibilità economica di questi attori del mercato.

A maggiori critiche si presta invece, come già osservato, la possibilità rimessa agli organismi notificati di adeguare le tariffe per la valutazione di conformità ad "altri indicatori pertinenti", considerato che, tali organismi, per quanto debbano essere indipendenti, mancano dei requisiti di terzietà e imparzialità necessari per una valutazione effettivamente ragionevole.

Ciononostante, dalla − per quanto sommaria− rassegna sin qui esposta, non si può non notare che uno sforzo è stato fatto, ora occorrerà vedere come tali previsioni potranno trovare applicazione a quelle che − nella realtà dei fatti − sono la maggior parte delle imprese presenti sul suolo nazionale e verificare se in concreto le semplificazioni e gli incentivi previsti

[270] Cassazione Penale, Sez. III, sent. n. 14631/2024.

siano idonei e sufficienti a garantire una piena partecipazione al mercato delle PMI e delle *start-up*.

INTELLIGENZA ARTIFICIALE, LAVORO E PMI: RIFLESSIONI SU UN SISTEMA DI TUTELA.

Chiara Ciccia Romito

Dottoressa di ricerca in Lavoro Sviluppo e Innovazione, Università degli Studi di Modena e Reggio Emilia, Fondazione Marco Biagi

SOMMARIO: 1. PMI e Intelligenza Artificiale. - 2. Lavoro e IA: la procedimentalizzazione come tecnica di tutela. - 3. La procedimentalizzazione come tecnica di tutela nelle PMI. - 4. Conclusioni.

1. PMI e Intelligenza Artificiale.

Il contributo che segue intende proporre una riflessione sulla logica di integrazione delle tutele e sul grado di complessità gestionale dei nuovi obblighi derivanti dalla regolamentazione europea sull'IA, nonché sul bilanciamento tra gli interessi datoriali e le necessità di tutela dei lavoratori, dal peculiare punto di vista del lavoro svolto nelle piccole, medie e microimprese (PMI).

Le PMI costituiscono il 99 % delle imprese dell'UE: forniscono due terzi dei posti di lavoro nel settore privato e contribuiscono a più della metà del valore aggiunto totale creato dalle imprese dell'Unione europea[271]. In Italia, nel 2019 le imprese dell'industria e dei servizi di mercato si confermano in prevalenza di piccolissima dimensione (1-9 addetti). Le microimprese sono, infatti, quasi 4 milioni e rappresentano il 94,8 per cento delle imprese attive, il 43,2 per cento degli addetti e solo il 26,8 per cento del valore aggiunto complessivo. Le grandi imprese (250 addetti e oltre) sono lo 0,1 per cento del totale delle imprese, assorbono il 23,3 per cento dell'occupazione e creano il 35,3 per cento di valore aggiunto. A livello nazionale, pertanto, il 95,2 per cento delle imprese manifatturiere sono imprese di piccole dimensioni (massimo 9 addetti) che impiegano il 43,2 per cento degli addetti totali. Percentuali più alte si registrano nei settori degli altri servizi, con il 97,7 per cento di imprese e il 48,1 per cento di addetti, e delle costruzioni, con il 95,7 per cento di imprese e il 62,1 per cento di addetti[272].

Con il ricorso, sempre più diffuso, alle nuove tecnologie, le PMI si trovano sempre più coinvolte nella raccolta, elaborazione e conservazione di dati particolari, sia riguardanti i propri dipendenti che i clienti e i fornitori. In questo contesto, è essenziale garantire un

[271] Cfr. Parlamento europeo, *Note Tematiche sull'Unione Europea*, aprile 2023, https://www.europarl.europa.eu/factsheets/it/sheet/63/piccole-e-medie-imprese.
[272] Istat, Annuario Statico Italiano: Imprese, https://www.istat.it/, 28 luglio 2022.

adeguato livello di sicurezza dei dati per prevenire rischi legati alla violazione della riservatezza e alla sicurezza delle informazioni. Inoltre, la capacità di adottare tecnologie digitali influenzerà la competitività, la produttività e la sostenibilità delle PMI nel panorama economico attuale. In tale scenario diventa fondamentale porre l'attenzione sulle tutele del lavoro nelle piccole e medie imprese: l'adozione accelerata delle tecnologie digitali può richiedere una revisione delle attuali normative per garantire la protezione e l'equità in un ambiente lavorativo in evoluzione[273].

L'introduzione dell'automazione e dei dispositivi digitali all'interno degli ambienti lavorativi ha il potenziale di modificare le dinamiche interpersonali esistenti tra individui, considerando il carattere innovativo delle funzioni che le macchine si apprestano a ricoprire[274].

Per ottenere una visione complessiva e completa del quadro attuale è essenziale approfondire il grado di digitalizzazione in cui si trovano le PMI italiane. La valutazione delle loro capacità digitali risulta essenziale per identificare le modifiche organizzative necessarie al fine di adattarsi alle dinamiche del mercato del lavoro.

Le informazioni fornite derivano da un'indagine quantitativa condotta dall'Osservatorio Innovazione Digitale delle PMI presso il Politecnico di Milano, la quale ha permesso di delineare l'attuale quadro relativo alla digitalizzazione delle PMI[275].

La ricerca dell'Osservatorio ha indagato sul grado di maturità digitale delle PMI[276]. Il grado di maturità indica il livello di competenza con cui l'azienda implementa e utilizza le tecnologie digitali in conformità alle esigenze aziendali e alle strategie di sviluppo. Tale elemento riflette il grado in cui le tecnologie digitali sono integrate nei processi operativi, nella comunicazione interna ed esterna e nella gestione dei dati, consentendo all'organizzazione di trarre beneficio dalla digitalizzazione in termini di efficienza, innovazione e adattamento alle mutevoli dinamiche del mercato[277].

---

273 PASCUCCI F., TAMPERINI V., *Trasformazione digitale delle PMI*, *Approcci Strategici e strumenti operativi*, G. Giappichelli Editore, Torino, 2017, 72.

274 Secondo FAIOLI, le macchine rivestiranno il ruolo di terzo elemento nella fabbrica intelligente. *L'oggetto del contratto di lavoro andrà oltre le mansioni identificate ex ante, in fase di costituzione del rapporto di lavoro.* FAIOLI M., *Mansioni e Macchina Intelligente*, Giappichelli, Torino, 2018, 211.

275 Politecnico di Milano, *Osservatorio Innovazione Digitale delle PMI, la Maturità digitale delle PMI italiane: dove siamo arrivati?, ricerca report 2022- 2023*, a cura del Gruppo di Lavoro composta da RANGONE A. , RORATO R., F. IANNELLA F., RE N., LOMBINI S., PARISI F. Copyright in capo al DIG, Dipartimento ingegneria Gestionale del Politecnico di Milano.

276 L'analisi si è basata su un campione di 1074 PMI.

277 *La capacità di un'istituzione di utilizzare, gestire, creare e comprendere il digitale, in modo contestuale (adatto al proprio ambiente e alle proprie esigenze specifiche), olistico (che coinvolge la visione, la leadership, il processo, la cultura e l'organizzazione) e propositivo (costantemente allineato alla missione dell'istituzione),* FINNIS J.*, The Digital Transformation Agenda and GLAMs: A Quick Scan Report for Europeana,* 2020.

Indagare sulla maturità digitale delle piccole e medie imprese implica la considerazione di vari fattori, sia interni che esterni all'azienda. Tali fattori possono essere suddivisi in tre categorie principali: la cultura digitale e il livello di competenze digitali all'interno dell'impresa; il grado di digitalizzazione dei processi aziendali, sia quelli primari legati alla produzione di beni o servizi, sia quelli di supporto come acquisti, marketing, vendite, contabilità; e infine, la capacità di collaborare con attori esterni per la realizzazione di progetti di trasformazione digitale, inclusi partner quali startup, enti di trasferimento tecnologico, e l'accesso a finanziamenti pubblici.

Sulla base dell'indice di maturità digitale sviluppato dall'Osservatorio, è possibile procedere alla categorizzazione delle PMI italiane in quattro distinti profili. Risulta che una percentuale inferiore al 50% di tali imprese rientra nei profili definiti come "convinto" (36%) o "avanzato" (9%). In contrasto, la restante percentuale, pari al 55% delle PMI, manifesta una tendenza a adottare atteggiamenti "timidi" (39%) o "scettici" (16%) in relazione alla trasformazione digitale.

In particolare, il segmento delle PMI con atteggiamenti "scettici" rappresenta un 16% del totale. Tale segmento si caratterizza per una certa reticenza verso l'ambito digitale che si manifesta attraverso l'assenza di consapevolezza circa i benefici offerti dalle tecnologie digitali, la carenza di competenze interne e/o di una struttura organizzativa in grado di agevolare in modo idoneo il processo di digitalizzazione, nonché l'implementazione di soluzioni digitali all'interno dei processi operativi. Inoltre, la carenza di un approccio olistico in campo digitale è associata a una minor predisposizione a interagire con soggetti esterni, quali enti di trasferimento tecnologico, attori della filiera produttiva e la Pubblica Amministrazione, allo scopo di sviluppare progetti di trasformazione digitale.

L'analisi dei dati relativi all'indice di maturità digitale delle PMI italiane, elaborato dall'Osservatorio, offre una visione interessante del panorama attuale. Emerge inequivocabilmente una considerevole proporzione di imprese che, nonostante gli sforzi profusi e l'accresciuta attenzione verso il processo di digitalizzazione, dimostra di trovarsi ancora in una fase iniziale o di manifestare scetticismo nei confronti di tale trasformazione digitale.

Particolarmente significativo risulta l'andamento del 55% delle PMI, il quale manifesta una tendenza verso una maturità digitale più cauta o addirittura scettica. Tale scenario potrebbe suggerire l'esistenza di ostacoli o di barriere che inibiscono tali imprese dal cogliere appieno le opportunità intrinseche nelle tecnologie digitali, nonostante la riconosciuta rilevanza della digitalizzazione.

I dati mettono in luce un divario tra le PMI che dimostrano una maturità digitale più spiccata e quelle che mostrano una certa reticenza. La discrepanza rilevata dalla ricerca potrebbe suggerire l'esistenza di differenze relative alla consapevolezza, alla formazione delle competenze e alle strategie aziendali che caratterizzano le due categorie.

I risultati dell'analisi svolta dall'Osservatorio forniscono un quadro interessante, altresì in riferimento alle percezioni delle PMI italiane in merito alla digitalizzazione. Emergono delle tendenze distinte all'interno del panorama imprenditoriale, riflettendo la diversificazione delle prospettive in materia. I dati rivelano che un rilevante gruppo di aziende ha adottato un approccio proattivo verso la digitalizzazione e sta sperimentando i conseguenti vantaggi. Al contempo, si osserva una distinzione tra le imprese che individuano nel digitale una componente già presente nel loro contesto operativo (25%) e coloro che invece lo considerano marginale (35%). Quest'ultima categoria sembra indicare una carenza di consapevolezza sulla pervasività del digitale e sui suoi impatti sui processi aziendali e le relazioni interne ed esterne. Come osservato nel report, l'elevato numero di imprese che percepisce il digitale come marginale potrebbe riflettere un livello di cultura digitale meno sviluppato.

Inoltre, va rilevato che quasi il 40% delle PMI manifesta una visione limitata degli impatti effettivi della digitalizzazione. Le aziende potrebbero considerare i costi associati alla digitalizzazione come eccessivi o potrebbero non avere una comprensione completa dei benefici che tale processo può comportare. Tale dato enfatizza la necessità di un'educazione più approfondita sulla digitalizzazione, al fine di assistere tali imprese nella valutazione accurata dei costi e dei benefici.

L'analisi compiuta dall'Osservatorio svela una panoramica articolata delle percezioni delle PMI italiane sul tema. I risultati sottolineano la complessità delle dinamiche e degli atteggiamenti all'interno dell'ambito imprenditoriale, con distinte sfaccettature di approcci e posizioni.

L'effetto positivo della trasformazione digitale sulle imprese delle PMI è stato rilevato da una recente ricerca pubblicata nell' International Journal of Information Management[278]. Tale studio evidenzia chiaramente come l'adozione di soluzioni digitali abbia il potenziale di migliorare significativamente le performance e la competitività delle PMI. Secondo lo studio delle analisi quantitative citate, la tecnologia agisce da forza motrice per la competitività delle

[278] SKARE M., DE LAS MERCEDES DE OBESSO M., RIBEIRO-NAVARRETE S., *Digital transformation and European small and medium enterprises (SMEs): A comparative study using digital economy and society index data, International Journal of Information Management*, n. 68, 2023.

PMI, fornendo strumenti e risorse che potenziano l'innovazione, l'efficienza e la capacità di adattamento.

Stando ai dati riportati, la trasformazione digitale, pertanto, non rappresenta solo un cambiamento – ormai avvenuto – ma al contrario una strada necessaria per garantire la competitività.

In un'ottica pragmatica, l'attuale condizione delle piccole e medie imprese richiede di avviare processi di digitalizzazione all'interno di un contesto in cui la mentalità dovrebbe essere orientata al digitale. Tale orientamento, dovrà tenere in considerazione, altresì, la natura del nuovo rischio intelligente: non immediatamente percepibile e complesso da comprendere.

La tecnica normativa impiegata dal Legislatore nell'AI ACT segue la linea tracciata dal GDPR, adottando un approccio basato sul rischio. La metodologia, pur non essendo innovativa, enfatizza la sostanza dell'adempimento e introduce il concetto di responsabilità, o accountability, come risultato di una rendicontazione continua. In altre parole, l'adempimento richiede una verifica costante e documentata della conformità, che evidenzia la capacità delle organizzazioni di gestire i rischi associati.

Tale approccio trova applicazione anche nella normativa italiana, in particolare nel Decreto Legislativo 81/2008 e nell'art. 2087 del Codice civile in materia di salute e sicurezza sui luoghi di lavoro. La chiave di volta è la responsabilizzazione degli attori coinvolti, tenuti a dimostrare di aver adottato tutte le misure necessarie per prevenire e mitigare i rischi. Il fulcro di tale approccio richiama la necessità di un'attenzione dinamica, che nel contesto lavorativo implica l'applicazione di più normative. Tali normative, pur tendendo a finalità diverse, costituiscono parte integrante del processo di compliance.

L'approccio dinamico si basa sulla capacità delle organizzazioni di adattarsi costantemente ai cambiamenti normativi e ai nuovi rischi emergenti. Nel contesto lavorativo, ciò si traduce nell'applicazione simultanea e integrata di diverse normative che, pur mirando a obiettivi specifici distinti – protezione dei dati personali, regolamentazione delle tecnologie di intelligenza artificiale e sicurezza sul lavoro – concorrono tutte al raggiungimento di un ambiente di lavoro sicuro. In tal modo, la compliance è costituita da un processo olistico che richiede un'attenzione continua e una gestione proattiva. In sintesi, l'approccio basato sul rischio e basato sul concetto di accountability richiede l'adozione di una cultura organizzativa orientata alla prevenzione. L'introduzione dei sistemi intelligenza artificiale nelle piccole e medie imprese comporta una serie di sfide, tra cui la necessità di adeguarsi all'AI ACT, nel quale il rischio si discosta da quello tradizionale poiché complesso e proteiforme.

Ulteriormente, la gestione integrata del rischio che porta a una procedimentalizzazione come tecnica di tutela deve essere inserita in un contesto tradizionalmente legato alle logiche di semplificazione normativa e burocratica.

2. Lavoro e IA: la procedimentalizzazione come tecnica di tutela.

Le modalità tramite le quali il datore di lavoro è tenuto a proteggere gli interessi dei lavoratori nel sistema dell'AI ACT si estrinseca principalmente in quattro tipi di tutele: sorveglianza, trasparenza, integrità e sicurezza.

Il livello di interconnessione e comunicazione nella fabbrica intelligente richiede un'adeguata procedimentalizzazione degli adempimenti a valle degli standard fissati a livello normativo. Le interazioni tra uomo e macchina[279], così come le comunicazioni tra le macchine stesse, sono, infatti, regolate da procedure che mirano a garantire non solo l'efficienza e la sicurezza operativa, ma anche la conformità a standard etici e giuridici. Lo scopo è quello di garantire un monitoraggio che consenta di esercitare una signoria sul sistema, "tradurre" il linguaggio del sistema e interromperlo qualora necessario a seguito di un'attività di sorveglianza umana[280] imposta dall'AI ACT al Deployer (datore di lavoro)[281].

L'orientamento normativo si traduce nella determinazione di una serie di adempimenti scanditi da procedure basate su un'analisi del rischio del sistema intelligente. Il rischio nell'IA ACT, come già osservato nel precedente paragrafo, dipende dal contesto di implementazione e dai dati raccolti dal sistema e si riferisce alla probabilità che l'uso di sistemi di intelligenza

[279] La rapida evoluzione delle tecnologie digitali ha catalizzato una trasformazione radicale del lavoro, in particolare nelle cosiddette "fabbriche intelligenti", dove il lavoro si configura come un "atto linguistico performativo". In questi contesti avanzati, caratterizzati da un modello organizzativo che produce attraverso la comunicazione, si verifica un'intensa interazione tra persone, oggetti e macchine intelligenti, delineando un panorama di comunicazione multilivello: uomo/uomo (H2H), macchina/macchina (M2M) e uomo/macchina (H2M). In questo scenario, l'acronimo M2H descrive una tecnologia intelligente e interconnessa che facilita una comunicazione machine-to-human continua e interattiva, sfruttando dispositivi di visualizzazione, sensori in rete e allarmi, per realizzare un processo collaborativo e correttivo uomo-macchina, volto a garantire il funzionamento ottimale di un sistema produttivo. Questa organizzazione, che produce comunicando attraverso sensori IoT integrati in dispositivi connessi in rete, può essere un macchinario, un nastro trasportatore, un sollevatore o un'intera fabbrica. Le soluzioni basate sulla comunicazione M2H sono progettate per rilevare precocemente stress, errori o imperfezioni, e prevedere guasti di dispositivi o apparecchiature. MARI G., *Il lavoro 4.0 come atto linguistico performativo. Per una svolta linguistica nell'analisi delle trasformazioni del lavoro*, in CIPRIANI A., GREMOLATI A., MARI G. (a cura di), Il lavoro 4.0: la quarta rivoluzione industriale e la trasformazione delle attività lavorative, Firenze University Press, 2018.

[280] Art. 26 par 2 dell'AI ACT dispone I deployer affidano la sorveglianza umana a persone fisiche che dispongono della competenza, della formazione e dell'autorità necessarie nonché del sostegno necessario. Ma si pensi anche alla richiesta di accesso ai sensi del GDPR o all'esercizio della trasparenza come previsto dal D.lgs. 104/2022. In ogni caso, la richiesta implica una revisione, e quindi, un'eventuale "blocco" dell'attività svolta. Cfr. *amplius* le considerazioni di PALMIROTTA F. in questo Volume.

[281] Il Considerando 16 dell'AI ACT dispone "La nozione di deployer di cui al presente regolamento dovrebbe essere interpretata come qualsiasi persona fisica o giuridica, compresi un'autorità pubblica, un'agenzia o altro organismo, che utilizza un sistema di IA sotto la sua autorità, salvo nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale. A seconda del tipo di sistema di IA, l'uso del sistema può interessare persone diverse dal deployer".

artificiale possa generare danni o impatti negativi su persone, beni o processi. Esso si declina in diverse dimensioni.

Il rischio tecnologico, innanzitutto, concerne la possibilità che il sistema di IA operi in modo non conforme alle aspettative, causando decisioni o azioni errate.

Il rischio di sicurezza riguarda la vulnerabilità del sistema di IA a cyberattacchi, accessi non autorizzati e altre forme di compromissione della sicurezza informatica. Un sistema esposto a tali minacce può essere manipolato con finalità malevole, pregiudicando l'integrità dei dati e la sicurezza complessiva delle operazioni.

Infine, il rischio etico rappresenta un ulteriore livello di criticità, con implicazioni che spaziano dai bias algoritmici alla discriminazione automatizzata.

Nella gestione del rischio, il datore di lavoro deve tenere conto degli obblighi imposti da diverse fonti normative che, pur con le loro differenze, presentano significative affinità con il modello e principi regolativi dell'AI ACT.

In questo contesto, il GDPR impone, tramite il principio di accountability, una rendicontazione continua delle operazioni di trattamento dei dati, sia *ex ante* che *ex post*. Conseguentemente, si instaura un processo di valutazione e revisione costante che coinvolge tutti gli aspetti del trattamento dei dati. Analogamente, l'articolo 22 del GDPR richiede una revisione umana dei processi decisionali automatizzati e stabilisce l'obbligo di una valutazione umana delle decisioni automatizzate[282].

Anche l'art. 4 dello Statuto dei lavoratori assume la procedimentalizzazione come *modus operandi* e si estende alla base dello stesso processo di implementazione dello strumento intelligente[283]. Gli strumenti di intelligenza artificiale, per loro natura, operano un monitoraggio costante dell'attività lavorativa. Il monitoraggio è parte del processo di implementazione dello strumento stesso e implica la raccolta e l'elaborazione di dati che sottostanno al rispetto delle tutele statutarie.

---

[282] 1. 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. 2. Il paragrafo 1 non si applica nel caso in cui la decisione: a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento; b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato; c) si basi sul consenso esplicito dell'interessato. 3. Nei casi di cui al paragrafo 2, lettere a) e c), il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione. 4. Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.

[283] *Tutti i sistemi di IA, date le caratteristiche e potenzialità rientrano sempre e necessariamente – nell'alveo del comma 1 del "nuovo" art. 4, l. n. 300/1970, non potendo mai costituire dei meri strumenti di lavoro ai sensi del comma 2.* Così IMBERTI L., *Intelligenza artificiale e sindacato. Chi controlla i controllori artificiali, federalismi.it* -n. 29/2023.

La Direttiva sul lavoro da piattaforma, da parte sua, estende ulteriormente questa necessità di revisione umana, stabilendo un diritto esplicito al controllo umano sui processi decisionali automatizzati[284].

Il Decreto Trasparenza, al contempo, impone la necessità di comprendere a fondo il sistema di decisionale e di monitoraggio automatizzati per spiegare la logica delle sue funzionalità. Conseguentemente, i processi automatizzati devono essere trasparenti, ma altresì comprensibili agli utenti e ai soggetti interessati.

Infine, il Regolamento sull'Intelligenza Artificiale pone il rischio al centro del suo stesso approccio, affidando ai datori di lavoro l'obbligo di un monitoraggio attento, costante e specializzato[285].

La procedura non è soltanto un insieme di passaggi formali, ma rappresenta una specifica tecnica regolativa attraverso la quale le tutele necessarie a seguito dello sviluppo tecnologico vengono identificate e interpretate. La digitalizzazione, infatti, comporta la creazione di un'infrastruttura di coordinamento che richiede la presenza di una governance e un insieme di misure e politiche tese a garantire l'effettività delle tutele[286]. Tale infrastruttura necessita dell'interazione di vari soggetti con diverse competenze, che variano dalle responsabilità esecutive e direttive a ruoli consultivi e informativi.

Trasparenza, spiegazione e il riesame umano di decisioni prese automaticamente richiedono espressioni linguistiche che devono essere codificate in un testo. Il testo deve, poi, essere collocato all'interno di un contesto e reso comprensibile al destinatario, che

[284] La Direttiva introduce meccanismi di protezione, quali la sorveglianza umana e la sicurezza nell'applicazione di processi algoritmici nella gestione del lavoro su piattaforme digitali. Secondo la Direttiva l'utilizzo di una piattaforma di lavoro digitale presuppone di per sé l'impiego di sistemi automatizzati per il processo decisionale o il monitoraggio, e apporta una maggiore precisione nel definire come il lavoro sia organizzato e valutato. La Direttiva prevede un obbligo di controllo umano sui sistemi automatizzati utilizzati dalle piattaforme di lavoro digitale e quello di compiere una valutazione d'impatto, con frequenza biennale, sull'effetto di queste decisioni automatizzate sui lavoratori. L'attività deve prevedere il coinvolgimento dei rappresentanti dei lavoratori, sia nella fase iniziale di svolgimento della valutazione sia in quella finale di adozione delle misure nel caso in cui la valutazione abbia definito un alto rischio.

[285] L'art. 26 stabilisce: I deployer affidano la sorveglianza umana a persone fisiche che dispongono della competenza, della formazione e dell'autorità necessarie nonché del sostegno necessario.
3. Gli obblighi di cui ai paragrafi 1 e 2 lasciano impregiudicati gli altri obblighi dei deployer previsti dal diritto dell'Unione o nazionale e la libertà del deployer di organizzare le proprie risorse e attività al fine di attuare le misure di sorveglianza umana indicate dal fornitore. 4. Fatti salvi i paragrafi 1 e 2, nella misura in cui esercita il controllo sui dati di input, il deployer garantisce che tali dati di input siano pertinenti e sufficientemente rappresentativi alla luce della finalità prevista del sistema di IA ad alto rischio. L'art. 26 dell'AI ACT prevede Prima di utilizzare un sistema di IA ad alto rischio di cui all'articolo 6, paragrafo 2, ad eccezione dei sistemi di IA ad alto rischio destinati a essere usati nel settore elencati nell'allegato III, punto 2, i deployer che sono organismi di diritto pubblico o sono enti privati che forniscono servizi pubblici e i deployer di sistemi di IA ad alto rischio di cui all'allegato III, punto 5, lettere b) e c), effettuano una valutazione dell'impatto sui diritti fondamentali che l'uso di tale sistema può produrre.

[286] A cui vanno ad aggiungersi gli ulteriori adempimenti a cui l'Azienda è già obbligata e che creano un onere di compliance già esistente. Si pensi agli obblighi derivanti dal D.lgs. 81/2008, a quelli del D.lgs. 23/2024 che ha imposto una procedura di segnalazioni degli illeciti a tutte le aziende con almeno 50 dipendenti e agli oneri che derivano dall'eventuale applicazione dei processi 231/2001.

dovrebbe essere in grado di interpretarlo, controllarlo e giustificarlo sfruttando le proprie facoltà umane. Pertanto, nel contesto lavorativo, il diritto alla trasparenza delle condizioni di lavoro, all'accesso a informazioni "umanizzate" di terza generazione, alla spiegazione di decisioni automatizzate e al controllo e riesame umano, consolida prospetticamente il modello antropocentrico di intelligenza artificiale promosso dalle istituzioni europee[287]. Finalità a cui le procedure interne, per la compliance normativa, tendono.

La costruzione dell'informazione diventa procedura, e la sintesi tra l'insieme delle norme crea la necessità di una governance partecipativa e dinamica.

Tale dinamicità viene ripresa anche dall'accordo quadro delle parti sociali europee sulla digitalizzazione, che delinea la creazione di un processo circolare e dinamico e gestito congiuntamente quale modalità adeguata all'attuazione dei principi sostanziali dell'accordo, nel rispetto dei ruoli e delle responsabilità dei diversi attori alla base del fenomeno della digitalizzazione[288].

L'art. 26 par 7 dell'AI ACT prevede una consultazione con le rappresentanze sindacali[289], l'art. 35 del GDPR nella valutazione d'impatto prevede misure di consultazione[290], la Direttiva sulle piattaforme pone la consultazione come l'architrave funzionale all'informazione dei lavoratori, il Decreto trasparenza richiama la necessità di una consultazione con le rappresentanze sindacali così come l'art. 4 dello Statuto dei lavoratori prevede un accordo, prima dell'installazione dello strumento, e in assenza di rappresentanze, un'autorizzazione da parte dell'ente amministrativo deputato. In questa configurazione, le rappresentanze sindacali sono chiamate a svolgere un ruolo dinamico, che si colloca all'interno di una struttura collaborativa e circolare definita dall'accordo stesso incidendo, come visto, sulla governance stessa.

---

[287] ZAPPALÀ L., *Appunti su linguaggio, complessità e comprensibilità del lavoro 4.0: verso una nuova procedimentalizzazione dei poteri datoriali* WP C.S.D.L.E. "Massimo D'Antona" IT – _462/2022, 2022.

[288] Il testo dell'Accordo quadro europeo è disponibile in https://www.etuc.org/system/files/document/file2020-06/Final%2022%2006%2020_Agreement%20on%20Digitalisation%202020.pdf. Per un primo commento v. PIGNI G., *European Social Partners Framework Agreementon digitalisation: ottimizzare i benefici ed affrontare insieme le sfide della digitalizzazione*, *BA*, 2020, n. 26. V. anche il mio saggio su *ILLeJ*, n. 2/2020.

[289] Il paragrafo 7 dell'art. 26 dispone che Prima di mettere in servizio o utilizzare un sistema di IA ad alto rischio sul luogo di lavoro, i deployer che sono datori di lavoro informano i rappresentanti dei lavoratori e i lavoratori interessati che saranno soggetti all'uso del sistema di IA ad alto rischio. Tali informazioni sono fornite, se del caso, 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.

[290] L'art. 88, del GDPR sottolinea la necessità di salvaguardare la dignità del lavoratore, va letto in parallelo. In questo quadro, la partecipazione dei lavoratori nella valutazione d'impatto ai sensi dell'art. 35 GDPR si configura come un meccanismo di protezione, assicurando che le implicazioni dei sistemi vengano esaminate in modo inclusivo. Secondo la dottrina, il Regolamento impone che la consultazione debba essere sistematicamente effettuata durante la valutazione dei rischi associati all'esercizio del potere di controllo del datore di lavoro, un aspetto che deriva direttamente dai processi decisionali automatizzati. Si veda INGRAO A., *Il controllo a distanza sui lavoratori e la nuova disciplina privacy, una lettura integrata*, Cacucci Editore, Bari, 2018.

L'impostazione legislativa indica una preferenza per un modello di cooperazione e di revisione costante, sia nel sistema di gestione che nei processi comunicativi, sia all'interno della governance aziendale. Il flusso comunicativo messo in evidenza dalla normativa analizzata evidenzia, altresì, l'importanza della governance nel ciclo informativo di gestione del processo intelligente.

In tale disegno, l'informazione assurge ad elemento fondamentale attraverso il quale i rappresentanti prendono consapevolezza dei processi che riguardano il lavoro datificato e, tramite tale consapevolezza, esercitano l'azione a garanzia dei lavoratori. Tale diritto, espressamente riconosciuto dalla giurisprudenza di merito anche con riferimento alla normativa in materia di trasparenza[291], si inserisce nel contesto del rapporto di lavoro come presupposto fondamentale della consultazione e si pone in maniera strumentale all'esercizio dell'attività sindacale nell'organizzazione. La creazione di un sistema di garanzie procedurali, costruito per garantire la trasparenza avverso i rischi dell'IA, potrebbe portare ad un incremento delle protezioni legali nel sistema di governance e compliance precedentemente delineato. Secondo Treu, la previsione di poteri di controllo sulle scelte aziendali da parte delle rappresentanze dei lavoratori troverebbe la sua giustificazione nel principio costituzionale (art. 41) secondo cui l'iniziativa privata "non può svolgersi in contrasto con l'utilità sociale e in modo da recare danno alla sicurezza, alla libertà, alla dignità umana"[292].

Tuttavia, occorre operare una riflessione sulla categoria a cui è rivolta la presente trattazione: le piccole e medie imprese, infatti, sono in una posizione particolare, non sempre possono godere della struttura e della governance della grande impresa a causa di vari fattori come la dimensione dell'impresa, il settore di attività e la cultura aziendale. Inoltre, la stessa previsione statutaria all'art. 35 statuisce che le rappresentanze sindacali aziendali possono essere costituite solo all'interno di unità produttive che vedano impiegati più di 15 dipendenti nel caso di imprese industriali e commerciali e più di 5 per le imprese agricole. La ragione di tale perimetrazione si rinveniva nella classica struttura conflittuale dei rapporti all'interno dell'azienda.

Allo scopo di sollevare le PMI dai problemi derivanti da situazioni conflittuali non compatibili con la struttura della categoria, il Legislatore ha inteso adottare un criterio selettivo della macrocategoria imprenditoriale in grado di prevenire l'insorgere di tali situazioni[293]. Tuttavia, gli effetti dell'IA sono i medesimi in ciascun contesto imprenditoriale

[291] Tribunale di Palermo, 3 aprile 2023 RG n. 645/2023 e Tribunale di Torino Sentenza del 7 agosto 2023.
[292] TREU T., *La digitalizzazione del lavoro: proposte europee e piste di ricerca, federalismi.it,* n. 9/2022.
[293] DE LUCA TAMAJO R., art. 35, in G. GIUGNI (diretto da) *Lo statuto dei lavoratori commentario*, Giuffrè, Milano, 1979.

e, conseguentemente, anche le tutele apprestate dalle normative dovrebbero essere le medesime.

Infine, occorre precisare che la procedimentalizzazione si realizza in una gestione particolareggiata delle singole decisioni in materia di governance e compliance, in particolare quando si tratta di intelligenza artificiale e di sistemi decisionali automatizzati. La governabilità del sistema non è infatti misurabile in maniera preventiva e ogni processo è dotato di caratteristiche e rischi intrinseci che si differenziano a seconda del contesto di implementazione dello strumento intelligente. Ne discende la necessità di un'analisi sartoriale e su misura dell'impresa che non può essere generalizzata e relegata a forme di semplificazione normativa.

3. La procedimentalizzazione come tecnica di tutela nelle PMI.

La procedimentalizzazione, intesa come una tecnica volta a garantire l'effettività delle tutele, si presenta come necessaria nella fase attuativa dello strumento intelligente implementato nel contesto lavorativo. Che si tratti di una grande multinazionale o di una piccola impresa locale, l'impatto dell'IA sui processi aziendali, sulla gestione dei dati e sulle decisioni operative è identica. Le misure anche. Quindi, si presume che siano speculari le tutele.

Si deve riconoscere che nelle PMI, dove spesso mancano sistemi di governance maturi, personale specializzato e strutture organizzative robuste, il rispetto delle prescrizioni fissate dall'AI ACT potrebbe tradursi in un'affrettata corsa all'adeguamento che sfugge alla più elevata finalità della procedura stessa. Inoltre, la procedimentalizzazione implica l'esistenza di rappresentanze sindacali attive e di un dialogo consultivo e costruttivo che, nelle PMI, richiede un'architettura organizzativa che sia adeguatamente attrezzata per affrontare la complessità tecnologica.

La carenza di adeguate misure di sicurezza, che dovrebbero costituire il fondamento e la condizione stessa della digitalizzazione, può rappresentare un ostacolo. In altre parole, la gestione delle procedure rischia di gravare solo sull'imprenditore.

L'analisi del rischio eseguita *ex ante*, da cui poi si origina la stessa procedura, è un onere che incombe principalmente sul datore di lavoro. È il datore di lavoro che deve anticipare e valutare i rischi, stabilendo le misure preventive da integrare nelle procedure aziendali, un processo complesso che richiede una visione delle potenziali conseguenze sul lato del diritto e il lato della tecnica, e di come quest'ultima influenza il primo.

In un contesto organizzativo strutturato, la decisione di implementare un nuovo processo è idealmente il risultato di una deliberazione congiunta tra diversi soggetti, e si accompagna all'adozione di adeguate misure di sicurezza. La complessità dell'analisi del rischio in tali circostanze diviene particolarmente elevata. La valutazione del nesso causale, che deve essere svolta *ex ante*, prima dell'eventuale manifestazione di un danno, non elimina la responsabilità che potrebbe emergere *ex post*, in seguito a un evento dannoso. Piuttosto, una corretta gestione preventiva del rischio può minimizzare o persino eliminare la responsabilità per danni che potrebbero verificarsi successivamente, influenzando direttamente l'effettività delle tutele. Tale elemento è particolarmente rilevante quando si considera il rischio non solo in termini di eventi dannosi, ma anche come la potenziale lesione dei diritti "digitali" complessi e multidimensionali quali autodeterminazione e dignità dei lavoratori. In un ambiente aziendale in cui siano presenti rappresentanze sindacali, strutture IT, sussista un'organizzazione chiara dei ruoli e funzioni, dotata di DPO e supportato da consulenza esterna specialistica, anche se onerosa, la gestione del rischio può essere sistematica e integrata[294]. Tuttavia, per le PMI, che spesso operano senza questi ampi supporti, sorgono interrogativi riguardo l'adeguata gestione del rischio e la sua integrazione nei processi aziendali. D'altro canto, per i lavoratori della PMI, dove le strutture organizzative sono più snelle e i ruoli di governance non sempre ben definiti, e dove spesso manca la componente sindacale, il rischio è quello di trovarsi davanti ad una discriminazione del sistema che sul piano delle tutele fa dipendere la qualità della tutela all'ente di appartenenza del lavoratore. In conclusione, dunque, si apre una riflessione su come le PMI, dotate di risorse limitate, possano efficacemente sviluppare e gestire il sistema procedurale descritto, poiché è dall'insieme delle misure e dagli adempimenti analizzati che dipendono le tutele dei lavoratori.

4. Conclusioni.

La trasformazione tecnologica non deve essere interpretata semplicemente come un fenomeno che le piccole e medie imprese subiscono. Al contrario, è una necessità strategica che si impone per garantire la loro competitività e sostenibilità nel mercato attuale e futuro. La ricerca effettuata tramite la banca dati dell'Indice di economia e società Digitali (DESI) fornisce evidenze significative a supporto di questa affermazione[295].

[294] BARBERA M., *La nave deve navigare. Rischio e responsabilità al tempo dell'impresa digitale*, *LLI*, vol. 9, n. 2, 2023.

[295] SKARE M., DE LAS MERCEDES DE OBESSO M., RIBEIRO-NAVARRETE S., *Digital transformation and European small and medium enterprises (SMEs): A comparative study using digital economy and society index data, International Journal of Information Management*, n. 68, 2023. Questo studio è stato uno dei pochi approfonditi che ha fatto uso dell'Indice DESI (Indice dell'Economia e della Società Digitali) per esaminare l'impatto della trasformazione digitale sulle PMI europee, fornendo così un contributo significativo alla comprensione di questa relazione. La ricerca ha approfondito i vantaggi e svantaggi della trasformazione digitale per le PMI europee, fornendo dati

La progressione della tecnologia ha trasformato il tessuto operativo e strategico delle PMI, incidendo non soltanto sulla loro efficienza produttiva, ma anche sulle dinamiche di mercato e sulla stessa concezione di lavoro e di organizzazione aziendale.

Il riconoscimento della parità tecnologica tra imprese è un principio e una conseguenza fondamentale nel contesto dell'economia digitale; tuttavia, l'applicazione pratica di tale principio deve inevitabilmente tenere conto delle specificità delle piccole e medie imprese. La loro struttura organizzativa, dimensione ridotta e risorse limitate creano un insieme di condizioni che differenziano significativamente le PMI dalle grandi imprese, soprattutto in termini di capacità di adattamento ai cambiamenti tecnologici e agli adempimenti che ne conseguono.

Le PMI si trovano di fronte a un complesso scenario: da un lato, l'adozione di nuove tecnologie è essenziale per la sopravvivenza e la crescita in un mercato dominato dall'innovazione digitale; dall'altro, la complessità e il costo dell'implementazione di tali tecnologie (anche in riferimento agli adempimenti derivanti) possono risultare proibitivi.

Il concetto di semplificazione è da sempre accostato a quello di PMI. Nella sua accezione tradizionale la semplificazione normativa è sempre stata orientata verso la riduzione degli oneri amministrativi e la facilitazione degli adempimenti burocratici per le imprese. L'approccio adottato dal Legislatore nel passato si è sostanzialmente concretizzato in politiche di incentivazione fiscale e in una diminuzione degli ostacoli normativi. Tuttavia, il rapido avanzamento tecnologico ha reso tale modello di semplificazione potenzialmente obsoleto.

L'era della datafication, guidata dallo sviluppo e dall'adozione dell'intelligenza artificiale, produce effetti sostanziali su tutte le realtà aziendali, indipendentemente dalla loro dimensione o settore di attività. La pervasività di questi effetti e strumenti ha portato il Legislatore europeo alla necessità di governare le implicazioni dell'intelligenza artificiale prevedendo adempimenti specifici che non possono essere semplificati né omogeneizzati in maniera indiscriminata, data la necessità di garantire adeguati livelli di tutela.

A partire da questa considerazione, nasce la considerazione sulla tutela del lavoro. In Italia, il tessuto imprenditoriale è principalmente costituito da PMI, le stesse forniscono occupazione all'80% dei lavoratori dipendenti del Paese[296].

empirici in questo contesto. L'Indice DESI, utilizzato come strumento di valutazione, ha valutato la trasformazione digitale considerando vari aspetti, tra cui la connettività, il capitale umano, l'uso di Internet, l'integrazione delle tecnologie digitali e i servizi pubblici digitali. L'indice ha consentito una visione completa della trasformazione digitale in Europa e dei suoi effetti sulle attività delle PMI. Per condurre l'analisi sull'impatto della trasformazione digitale sulle attività aziendali delle PMI europee, è stato utilizzato il database dell'Indagine sull'Accesso al Finanziamento delle Imprese nella zona euro (SAFE).

[296] Le imprese attive presenti sul territorio italiano nel 2020 sono 4 milioni e 354 mila per un totale di 17 milioni

È evidente che l'efficacia delle tutele per i lavoratori dipenderà dalla corretta applicazione delle garanzie stabilite dal Legislatore. Pertanto, è fondamentale che le PMI dispongano degli strumenti necessari per implementarle efficacemente allo scopo di assicurare il riconoscimento dello status dei lavoratori e la tutela dei loro diritti

Gli effetti della trasformazione digitale devono essere uniformi, così come uniformi devono essere le tutele che ogni imprenditore, indipendentemente dalla categoria di appartenenza, è tenuto ad applicare.

Tuttavia, mentre i cambiamenti indotti dalla rivoluzione tecnologica nel mondo del lavoro potrebbero apparire omogenei a livello macro, le implicazioni pratiche variano significativamente in base alle caratteristiche delle diverse categorie di imprese.

Il Legislatore è chiamato a un intervento proattivo: non più un mero alleggerimento degli obblighi amministrativi, ma una riconsiderazione sostanziale delle semplificazioni normative, che dovrà tener conto degli obblighi imposti dall'AI ACT in tutti i contesti imprenditoriali che implementano sistemi di IA. Da tale capacità d'intervento dipenderà l'effettività e la qualità delle tutele del lavoro e dei lavoratori. La prospettiva di un intervento proattivo mira anche a plasmare l'architettura del bilanciamento tra gli oneri del datore di lavoro e i diritti dei lavoratori. Senza adeguato supporto, gli imprenditori delle PMI potrebbero ritrovarsi in una posizione di svantaggio rispetto alla complessità e ai costi associati a ciascun adempimento normativo che costituisce la nuova governance caratterizzata da una procedimentalizzazione attenta, aggiornata e costante.

138 mila addetti (Tavola 14.1 e Prospetto 14.1). Ad un aumento di circa 50 mila imprese è corrisposta una diminuzione di 300 mila addetti. Il maggior numero di imprese (l'80 per cento) è impiegato nei servizi, cui corrisponde il 68,3 per cento di addetti (quasi equamente distribuito tra i due settori di competenza). Nell'industria in senso stretto sono presenti l'8,8 per cento di imprese a cui corrisponde il 23,7 per cento degli addetti complessivi. Lombardia e Lazio sono le regioni con più imprese (rispettivamente 18,5 e 10,1 per cento) e addetti (24,4 e 10,7 per cento). Il maggior numero di imprese e addetti è presente nel Nord-ovest (28,9 e 34,7 per cento). *//www.istat.it/storage/ASI/2022/capitoli/C14.pdf* .

CONSIDERAZIONI CONCLUSIVE

Simone Scagliarini
Ordinario di Diritto costituzionale e pubblico nell'Università di Modena e Reggio Emilia

È una prassi alquanto diffusa nei Convegni quella di affidare le conclusioni ad uno studioso autorevole, che peraltro molte volte finisce per presentare una propria relazione sul tema, con cui magari enuncia il suo pensiero prescindendo dal dibattito congressuale. Nel mio caso, non ricorrendo il presupposto *de quo* e nell'impossibilità di chiedere a Chat GPT od altro sistema di IA di assumere il mio ruolo, con un esperimento che pure sarebbe risultato assai interessante, mi limiterò a trarre una sintesi di quanto emerso dalle relazioni e dagli interventi che si sono susseguiti, accompagnandola con qualche considerazione più generale sul contesto di transizione che stiamo attraversando.

Non si tratta di un'operazione semplice, anche a prescindere dai limiti personali di chi la compie: l'impatto dell'IA è stato analizzato nel corso del nostro incontro da prospettive differenti, offrendo al dibattito punti di vista eterogenei quanto ad impostazione e modalità di lettura del medesimo fenomeno. Il quale, infatti, al pari, più in generale, di altre tematiche correlate alla trasformazione digitale della società cui stiamo assistendo, presuppone un approccio interdisciplinare al fine di essere correttamente compreso ed inquadrato, stante la sua natura trasversale e indissolubilmente legata ad una rilevante componente tecnica. Ciò spinge inevitabilmente – e virtuosamente – al dialogo i vari settori nei quali la scienza giuridica si è andata specializzando, talora ergendo, specie in ambito accademico, veri e propri steccati, questi sì decisamente artificiali, tra singole discipline. Da qui la nostra scelta, come Comitato scientifico, di affidare tre relazioni (e diversi interventi) a studiosi di rami diversi del diritto, per cercare di restituire un'immagine per quanto possibile tridimensionale dell'argomento oggetto di studio.

Un tema che è tornato più volte nel corso della giornata è quello dei dati, che costituiscono il carburante che permette il funzionamento dell'IA, con particolare attenzione per quelli personali e per le problematiche emergenti in relazione alla necessità di una loro tutela. Al riguardo, non può sfuggire come il Regolamento UE sull'IA vada a completare (*rectius*, arricchire) quel *corpus* normativo europeo che si regge ora su tre pilastri: 1) il GDPR, il sostegno più risalente, come si vede bene dalla sua impostazione rivolta più con lo sguardo al passato che al presente[297], un atto geneticamente non al passo con i tempi e a cui i due anni

[297] Ho cercato di dimostrare l'inadeguatezza del GDPR a fronteggiare la società algoritmica, prima ancora che l'IA, in SCAGLIARINI S., *La tutela della privacy e dell'identità personale nel quadro dell'evoluzione tecnologica*, in *Consulta*

di non applicabilità successivi alla sua entrata in vigore non hanno certo giovato in questo senso. Sia Giovanni Gaudio, il quale benevolmente ha richiamato (soltanto due dei a mio avviso ben più numerosi) difetti del Regolamento in questione, sia Giovanni Riccio, che più severamente ne ha stigmatizzato la situazione di incertezza che esso in più occasioni ha generato e genera, hanno indicato alcuni limiti di questo Regolamento; 2) la *Strategie europea dei dati* e, soprattutto, gli atti che da essa sono originati, quali il *Data Governance Act*, il *Digital Market Act*, il *Digital Services Act* e il *Data Act*[298]; 3) per l'appunto, il Regolamento sull'Intelligenza Artificiale, cui abbiamo dedicato il seminario e che negli anni a venire impegnerà grandemente operatori economici, regolatori, Authorities, giurisprudenza e dottrina rispetto alle problematiche che non tarderanno a manifestarsi in riferimento alla sua applicazione.

Il complesso di questo *corpus*, in cui peraltro possono essere ricompresi anche altri atti normativi collegati a quelli citati[299], benché a mio avviso privi dello stesso valore fondante, dà vita ad una disciplina, necessariamente integrata ed auspicabilmente sistematica[300], del mercato digitale, che non è *un* mercato, altro e parallelo rispetto a quello fisico, reale, ma è *il* mercato, nel quale vivono le imprese, su cui abbiamo concentrato l'attenzione in questo seminario. Perché la dimensione *onlife*[301] non riguarda solo le persone fisiche ma anche gli operatori economici, che ormai contemporaneamente e senza soluzione di continuità – anzi spesso in forma integrata – vivono sia una dimensione virtuale che materiale, o, per dirla con le parole usate in precedenza da Giovanni Riccio, vivono già in un metaverso. L'esistenza di questo stesso sistema fa anche sì che oggi non si debba più ragionare (solo) in termini di tutela di un singolo diritto, come era per il GDPR rispetto alla protezione dei dati personali, ma che ci troviamo di fronte ad una vera e propria disciplina della società digitale europea[302], di valore sostanzialmente costituzionale[303], essendo vocata ad assicurare, in un contesto

OnLine, 2021, n. 2, 583 ss., cui mi permetto di rinviare.

298 Ovvero, rispettivamente, i Regolamenti UE 2022/868, 2022/1925, 2022/2065 e 2023/2854.

299 Come, per esempio, il Regolamento UE 1807/2018 sulla libera circolazione dei dati non personali, la direttiva UE 2022/2555 in tema di cybersicurezza (cd. direttiva NIS2) o il recentissimo Regolamento UE 2024/1183 in tema di identità digitale (cd. Regolamento eIDAS2).

300 Non a caso Iacopo Senatori ha parlato di un raccordo, che Giovanni Gaudio ha poi mostrato, anche graficamente, nelle sue slides, tra queste discipline. Il che spiega anche perché la Fondazione Marco Biagi che ci ospita abbia deciso di rinominare il proprio Osservatorio sulla Privacy, di cui ho l'onore di essere il coordinatore, in Osservatorio su Privacy, IA e nuove tecnologie.

301 Il riferimento è chiaramente alla felice e ormai celeberrima espressione coniata da FLORIDI L., *La quarta rivoluzione*, Raffaello Cortina, Milano, 2014, spec. 47 ss.

302 In questo senso si esprime PIZZETTI F., *Pizzetti: "Da Tallin all'IA Act, così l'UE costruisce la sua Costituzione digitale"*, in *Agenda Digitale*, 7 maggio 2024, laddove afferma che il "pacchetto regolatorio citato, tuttavia, il focus della regolazione UE si allarga proprio perché al centro non ci sono più i dati personali, e cioè la tutela di uno specifico diritto, ma la tutela della circolazione digitale dei dati, quale che sia il loro tipo. Dunque, al centro non vi è più la tutela di un diritto ma esplicitamente la tutela della società digitale europea".

303 Del resto, come scrive FROSINI T. E., *Costituzionalismo 2.0*, in ID., *Liberté, égalité, internet*, Editoriale Scientifica,

digitale senza alcun precedente, la garanzia di quei diritti e di quelle libertà che il costituzionalismo, nei suoi ormai tre secoli di storia, ha inteso affermare, allora, verso il potere pubblico, e che, nel momento attuale, devono con forza essere rivendicati e garantiti nei confronti di potenti soggetti privati che dominano il mercato, ovvero le cd. *Big Tech*[304].

Nessuna impresa, dunque, se è vero quanto ho detto poc'anzi, è esente dal porsi il tema di come evolversi in questa nuova dimensione che, in misura maggiore o minore, sta già interessando – e vieppiù lo farà – tutti gli attori del mercato. Neppure le micro, piccole e medie imprese sono esenti da questo processo, come del resto dimostra il dato fornito da Chiara Ciccia Romito circa il coinvolgimento nell'IA, vuoi come fornitori, vuoi come *deployer*, già oggi del 60% delle PMI. Certo, il Regolamento, cercando di tenere conto delle specificità di questa tipologia di imprese, ha previsto opportunamente misure di sostegno, delle quali ci ha ampiamente parlato Veronica Palladini, ma proprio il fatto che l'atto normativo abbia dedicato loro specifiche disposizioni dimostra come giocoforza anch'esse siano direttamente interessate. Insomma, l'IA impatta su tutte le imprese a prescindere dalla loro dimensione, dal settore merceologico in cui operano, dalla loro dislocazione territoriale, ecc.

Il tema della PMI porta con sé quello delle *sandboxes*, su cui si è intrattenuto Giovanni Riccio in particolare nella prospettiva della concorrenzialità, nella sua duplice accezione di concorrenzialità all'interno del mercato ma anche di concorrenzialità *tra* mercati, con riferimento ai delicati equilibri geopolitici sul tema dello sviluppo e della regolazione dell'IA, alla luce dei quali deve essere valutato il tanto proclamato primato mondiale dell'UE, privo in realtà di qualunque plusvalore sul piano giuridico, ma chiaro messaggio e mossa strategica sul piano politico.

Accennavo prima al venir meno della distinzione tra mercato tradizionale e mercato digitale, ma in realtà a cadere, nell'attuale contingenza storica, è anche la stessa dicotomia tra mercato e "non mercato". Nel mondo *onlife*, in sostanza, siamo sempre immersi – e, ancora una volta, sempre più lo saremo – anche in una dimensione commerciale permanente, essendo a portata di *click*, con dispositivi che mai ci abbandonano, l'acquisto di qualsivoglia bene o servizio, senza limiti geografici o di tempo.

Napoli, 2ª ed., 2019, 189, "la sfida che nel Ventunesimo secolo attende il costituzionalismo è, prevalentemente, quella riferita alla tecnologia, ovvero come dare forza e protezione ai diritti di libertà […] in un contesto sociale profondamente mutato dall'innovazione".

[304] Giacché, come aveva intuito con la consueta lucidità e lungimiranza S. RODOTÀ, *Una Costituzione per internet*, in *PD*, n. 3, 2010, 341, *Google* (ma il discorso ben potrebbe essere esteso ad altre società con analoghe caratteristiche) "non è soltanto una delle strapotenti società multinazionali. È un potere a sé, superiore a quello di un'infinità di Stati nazionali, con i quali negozia appunto da potenza a potenza […] Governa corpi, conoscenza, relazioni sociali". Sul tema, nella letteratura ormai vasta che si sta formando, mi limito a rinviare, per tutti, a BETZU M., *I baroni del digitale*, Editoriale Scientifica, Napoli, 2022.

Ebbene in un contesto di questo tipo, i diritti costituzionali, ivi comprese le tradizionali libertà, sono immediatamente interessati da un'evoluzione che costringe a una loro rilettura e ad una riflessione su come si possa continuare ad offrire loro una tutela efficace, anche mediante la stessa regolazione dei meccanismi di mercato: il ricorso alla legislazione *antitrust* a tutela della privacy, di cui il caso più noto, ma non certo isolato, è la vicenda che ha visto contrapposto *Facebook* all'Autorità nazionale per la concorrenza tedesca, è emblematico di quanto sto dicendo e non è certo casuale che uno dei cardini di quella disciplina della società digitale europea cui facevo poc'anzi riferimento sia il *Digital Market Act*; una normativa evidentemente rivolta a migliorare la concorrenza nel mercato, con un fine che travalica però la mera dimensione commerciale e mira alla creazione di un mercato in cui i diritti trovino spazio. È la sfida del costituzionalismo digitale[305], che pare essere stata colta dal Regolamento laddove, postulando uno sviluppo di questa tecnologia finalizzato al miglioramento del benessere degli uomini (Considerando n. 6[306]) e affermando, fin dalla sua prima disposizione, il criterio della *human-centered AI*, si pone nel solco di quel principio personalista, assai noto alla nostra tradizione costituzionale, proiettandolo nel contesto della società digitale[307]. L'approccio valoriale enunciato testualmente dall'art. 1 del Regolamento, che richiama, seppure con una formulazione tecnicamente non proprio felicissima, il rispetto dei principi, dei diritti e degli interessi consacrati nella Carta dei diritti fondamentali dell'UE, trova diretta espressione in numerose disposizioni successive, su cui si è ampiamente trattenuta la relazione di Noemi Miniscalco, e in particolare nella previsione di cui all'art. 5 dei sistemi di IA vietati, proprio in quanto ritenuti inaccettabili per il rischio (che in certi casi è in realtà una certezza) di compromettere quei principi fondamentali, ma anche in tutta la disciplina prudenziale che circonda i sistemi ad alto rischio, di cui al Capo III del Regolamento.

Paradigmatico esempio di incidenza dell'IA sui diritti è proprio il caso del lavoro, al centro, insieme all'impresa, del seminario odierno, specialmente grazie alla relazione di Giovanni Gaudio. Non è, infatti, per avventura che tra i sistemi ad alto rischio l'allegato III, al punto

[305] Ben sintetizzata da PIZZETTI F., *Pizzetti: "Un nuovo costituzionalismo per l'Ue digitale"*, in *Agenda Digitale*, 9 gennaio 2024, allorché afferma che "la società digitale richiede un nuovo costituzionalismo che sappia declinare i tradizionali diritti fondamentali degli esseri umani anche nel mondo digitale già riconosciuti nella UE".

[306] Il quale afferma testualmente che "Come prerequisito, l'IA dovrebbe essere una tecnologia antropocentrica. Dovrebbe fungere da strumento per le persone, con il fine ultimo di migliorare il benessere degli esseri umani".

[307] In tema, *ex plurimis*, si vedano CASONATO C., *Costituzione e intelligenza artificiale: un'agenda per il prossimo futuro*, in *Biolaw Journal*, n. 2, 2019, spec. 725, ove l'A. evidenzia come i principi delineati negli artt. 9, 33 e 41 Cost. "possono costituire un'efficace cornice entro cui inserire una regolamentazione dell'AI costituzionalmente orientata, che la indirizzi verso scopi di progresso scientifico, economico e sociale, oltre che di generale benessere"; e SIMONCINI A., *La dimensione costituzionale dell'Intelligenza Artificiale*, in G. CERRINA FERONI, C. FONTANA, E. C. RAFFIOTTA (a cura di), *AI Anthology. Profili giuridici, economici e sociali dell'intelligenza artificiale*, il Mulino, Bologna, 2022, 135 ss.

4, indichi quelli relativi alla selezione del personale e alla gestione dei lavoratori, quando non sono oggetto di divieto assoluto, come quelli che mirano a inferire le emozioni di una persona fisica nell'ambito del luogo di lavoro, di cui al paragrafo 1, lett. f) dell'art. 5. Così come appare rilevante che l'art. 2, al paragrafo 11, consenta all'Unione e agli Stati membri di introdurre "disposizioni legislative, regolamentari o amministrative più favorevoli ai lavoratori in termini di tutela dei loro diritti in relazione all'uso dei sistemi di IA da parte dei datori di lavoro", direttamente o permettendo alla contrattazione collettiva, finanche incoraggiandola in questo senso, di muoversi in tale direzione. Ciò comporta per i datori di lavoro un significativo impatto in termini di obblighi (*in primis* la valutazione di impatto), divieti e adempimenti finalizzati alla trasparenza circa la esistenza e le logiche decisionali del sistema di IA (onere, quest'ultimo, per la verità, comune anche a quelli a rischio limitato, stante la natura trasversale di esso su cui ha focalizzato la sua attenzione Noemi Miniscalco).

Gli interventi programmati ci hanno offerto una vasta panoramica di temi legati all'uso dell'IA nel lavoro, scendendo nel dettaglio di alcune questioni, che peraltro non esauriscono certo il catalogo delle problematiche che sotto questa prospettiva vanno ad aprirsi, ma semmai offre un primo spaccato della ricchezza e complessità del testo normativo che ci troviamo di fronte e delle microquestioni (non certo tali con riferimento alla loro importanza) che si prospettano in relazione ad ogni singola disposizione.

In questo senso, l'accento è stato posto, grazie all'intervento di Federica Palmirotta, sul tema della possibilità di discriminazione algoritmica nella gestione delle risorse umane, alla quale, invero, potremmo aggiungere anche quella nella fase di selezione: d'altra parte, è noto che nel nostro Paese la giurisprudenza sull'amministrazione algoritmica si è formata proprio sul concorso per la stabilizzazione dei docenti a valle della normativa sulla cd. buona scuola[308].

L'argomento della opacità algoritmica e della conseguente necessità di trasparenza, che evocavo prima, evidenziandone la natura trasversale, si pone invero in modo specifico allorché i sistemi di IA siano utilizzati sui luoghi di lavoro, facendo emergere la questione della consultazione e della rappresentanza dei lavoratori, su cui si è intrattenuta Ilaria Purificato. Ma già Giovanni Gaudio aveva parlato del ruolo del sindacato, che a ben vedere si inquadra nel più ampio contesto della tutela collettiva, prevista sulla carta dal GDPR ma ampiamente ignorata dagli Stati membri in relazione alla protezione dei dati personali, e che ha portato ad aggiungere, nell'art. 110 del Regolamento di cui trattiamo, questa disciplina tra quelle per la cui violazione la direttiva UE/2020/1828 prevede azioni collettive.

[308] Su questa vicenda giurisprudenziale assai nota mi limito a rinviare per tutti a SIMONCINI A., *Amministrazione digitale algoritmica. Il quadro costituzionale*, in CAVALLO PERIN R., GALLETTA D.-U. (a cura di), *Il diritto dell'Amministrazione pubblica digitale*, Giappichelli, Torino, 2020, spec. 11 ss.

Collegato al tema della trasparenza sull'uso di sistemi di IA è quello del potere datoriale di controllo (*rectius*, dei poteri datoriali aumentati, come ha detto Giovanni Gaudio), di fronte al quale l'impiego di questa tecnologia porta una rivoluzione in un ambito nel quale già oggi si stenta a trovare una efficace convergenza tra normativa in materia di protezione dei dati personali e disciplina lavoristica (*i.e.*, in particolare, la legge n. 300/1970). Ilaria del Giglio, con il suo intervento in questo ambito, ci ha così riportati al punto da cui siamo partiti, ovvero quello dei dati come la materia prima indispensabile per il "processo produttivo" dell'IA, evocando una volta di più lo stretto legame, di cui dicevo poc'anzi, tra questa normativa ed il GDPR, che per l'appunto continua ad essere un pilastro, per quanto magari un po' traballante, della regolazione della società digitale.

La riflessione odierna, alla luce di un dibattito che ho cercato di richiamare per sommi capi e con una sintesi quasi brutale, credo sia stata perciò molto utile. Perché è vero che già da mesi si sono poste in essere tante iniziative, sia divulgative che di carattere più strettamente scientifico, sul tema dell'IA, variamente declinato (cosa davvero insolita per un atto normativo che, ad oggi, attende ancora l'approvazione formale del Consiglio dell'Unione europea[309] e che diverrà applicabile decorsi 24 mesi dalla sua pubblicazione, la cui data è ovviamente futura e incerta), come è vero che si tratta di un dibattito non esente dall'essere oggetto di moda, spingendo tutti ad occuparsene quotidianamente (e sappiamo bene come anche la dottrina non sia nuova a seguire le mode!), così come, infine, non si può negare che persino il legislatore, pur non avendo (o forse proprio in quanto non ha) idee chiare sull'oggetto che sta maneggiando, sta inserendo l'IA ovunque, in atti normativi che intervengono sui settori più disparati[310]; tuttavia, non si può parimenti trascurare che si tratta di una questione davvero centrale, giacché ci troviamo di fronte ad una tecnologia realmente pervasiva, che non tarderà ad interessare tutti i settori ordinamentali, sollevando, come abbiamo appena percepito grazie al dibattito odierno in relazione al contesto lavoristico, una miriade di questioni da risolvere. Di modo che il diritto dell'informatica e delle nuove tecnologie, che oggi costituisce oggetto di corsi universitari denominati più o meno in questo modo (e anche chi scrive ne è titolare) e che ancora viene richiamato nella declaratorie di

[309] Nelle more della pubblicazione di queste Conclusioni, si è in realtà dato corso, il 21 maggio 2024, anche a questo passaggio, di modo che, per il perfezionamento dell'*iter*, manca oggi solo la pubblicazione in Gazzetta Ufficiale.

[310] Tra cui, per limitarci a qualche esempio, si possono ricordare l'art. 30, comma 1, del d. lgs. 31 marzo 2023, n. 36, recante il Codice dei contratti pubblici, ai sensi del quale "per migliorare l'efficienza le stazioni appaltanti e gli enti concedenti provvedono, ove possibile, ad automatizzare le proprie attività ricorrendo a soluzioni tecnologiche, ivi incluse *l'intelligenza artificiale* e le tecnologie di registri distribuiti" o il recentissimo d. lgs. 25 marzo 2024, n. 41, il cui art. 22, nel disciplinare giochi e scommesse a distanza, al secondo comma, fa riferimento a "misure informatiche, anche implicanti il ricorso a soluzioni di *intelligenza artificiale*" per la individuazione dei siti di gioco illegali (i corsivi sono miei).

alcuni settori scientifico-disciplinari di recente rinnovate, è in realtà una categoria effimera destinata a scomparire: non esiste un diritto dell'IA, perché l'IA incide su tutto l'ordinamento ed occuparsi dell'impiego di questa tecnologia nel diritto del lavoro è occuparsi *tout court* di diritto del lavoro.

Non solo, ma l'importanza di un dibattito sul tema deriva anche dalla necessità che anche la dottrina, in questa fase, assista il regolatore e promuova l'idea, sottesa all'adozione di questo Regolamento, che lo sviluppo di tale tecnologia deve essere indirizzato, non già subito (ad opera di quelle *Big Tech* cui facevo cenno in precedenza). In questo senso può diventare significativo il primato dell'UE nella regolazione, quale frutto dell'impostazione di un percorso, iniziato a Tallin con il Consiglio europeo del 2017, volto a cercare gli strumenti per guidare un cambiamento che promette di essere epocale. A condizione, però, di chiederci anzitutto, come ha molto opportunamente ricordato Giovanni Riccio, se il Regolamento ponga le domande corrette a tal fine, perché questo è il nodo cruciale, più ancora della primazia temporale in sé che, altrimenti, sarebbe priva di utilità. La tecnica legislativa utilizzata nell'atto non è delle migliori, perché diversi sono i passaggi non chiari, auspicabilmente almeno in parte risolvibili con l'intervento dei giuristi revisori, così come non poche sono le disposizioni generiche e i rinvii ai legislatori nazionali: in questo contesto il monitoraggio attento degli sviluppi tecnologici e regolativi è un dovere cui per l'appunto (anche) la dottrina non può abdicare.

Ben venga, allora, che un soggetto vicino al territorio come la Fondazione Marco Biagi organizzi eventi come quello odierno e si attrezzi, come sta facendo, in coerenza alla sua natura di ente votato specialmente alla Terza missione universitaria, per avviare e mantenere un dialogo con gli operatori del mercato, anche attraverso le già programmate iniziative formative. Del resto, le imprese devono investire in competenze e capitale umano non solo nel loro primario interesse, ma anche per uno specifico obbligo introdotto dall'art. 4 del Regolamento, ovvero quello di alfabetizzare il proprio personale perché sappia gestire i sistemi di IA nel contesto in cui questi devono essere utilizzati. Insomma, anche le imprese devono cercare di governare e non subire questa rivoluzione tecnologica, nella consapevolezza, come ricordavo prima, che non stanno allargando o modificando il proprio *core business* ma che stanno semplicemente adattandosi ai mutamenti del mercato.