SPECIALE DELLA SETTIMANA

IA e lavoro: cosa rientra nella gestione dei rapporti di lavoro e nei sistemi ad alto rischio? Quali cautele?

di **Chiara Delaini**

Lo scorso 14 maggio il Consiglio Europeo ha approvato il testo del nuovo Regolamento Europeo in materia di intelligenza artificiale, che stabilisce regole armonizzate in tutto il territorio dell'UE per la produzione, la messa a disposizione e l'utilizzo di software che facciano uso di algoritmi di IA, a tutela sia del mercato sia dei diritti riconosciuti dalla Carta dei Diritti Fondamentali dell'Unione Europea.
Il Regolamento stabilisce una classificazione dei sistemi di intelligenza artificiale, individuando chiaramente come "ad alto rischio" quelli applicati nei principali processi di gestione delle risorse umane, lungo tutto il ciclo di vita degli stessi.
Nelle pagine che seguono l'autrice analizza le principali implicazioni in materia non solo di produzione, bensì di utilizzo di sistemi di questo tipo nel contesto del lavoro in Italia, tenendo in considerazione anche le prescrizioni già vigenti in materia di trasparenza e di sorveglianza umana, anche e soprattutto in presenza di decisioni automatizzate o sistemi di controllo a distanza.

IA e lavoro: un tema di etica e di rispetto della Carta dei Diritti Fondamentali

Per poter parlare di intelligenza artificiale applicata al rapporto di lavoro, tanto subordinato quanto "atipico", è necessario fissare alcuni concetti essenziali, di natura prima tecnologica e poi normativa, per perimetrare lo spazio entro il quale effettuare considerazioni e prendere decisioni. La materia, infatti, richiede la conoscenza non solo del dettato del recentissimo Regolamento sull'intelligenza artificiale e delle sue implicazioni su tutto il territorio dell'Unione Europea, ma anche della normativa in materia di protezione dei dati personali, sempre di respiro europeo, e del dettato nazionale ed estremamente rilevante non solo dello Statuto dei Lavoratori, ma anche del Decreto Trasparenza, veicolo delle regole irrinunciabili di informazione per la tutela dei diritti sul lavoro.

Per di più, lavorare con l'intelligenza artificiale e applicarla al rapporto di lavoro significa non solo destreggiarsi tra tecnologia e normativa, bensì tenere sempre presente l'etica come principio guida di tutte le decisioni e valutazioni effettuate: utilizzare algoritmi "intelligenti" a contatto con le persone espone i singoli individui (e quindi potenzialmente l'intera umanità) a rischi di violazione di ciò che abbiamo definito come nostri diritti fondamentali.

Per questo è necessario che l'uso che facciamo di questi strumenti tenga sempre in

considerazione le potenziali conseguenze sulla libertà e sulla dignità umana (in questo caso dei lavoratori): non più tardi di qualche anno fa, infatti, nella risoluzione 2020/2012(INL) del 20 ottobre 2020, lo stesso Parlamento Europeo ha rilevato che l'applicazione dell'intelligenza artificiale, della robotica e delle tecnologie correlate sul luogo di lavoro può contribuire a mercati del lavoro inclusivi e avere un impatto sulla salute e sulla sicurezza sul lavoro, ma nel contempo può essere utilizzata anche per monitorare, valutare, prevedere e orientare le prestazioni dei lavoratori, con conseguenze dirette e indirette sulla loro carriera.

Dando per note, quindi, le norme che stabiliscono le modalità e i requisiti di trasparenza necessari in Italia per l'implementazione di sistemi di valutazione e decisione automatizzata nel contesto del lavoro (con particolare attenzione ai sistemi di controllo a distanza), in questo articolo facciamo un approfondimento sul dettato normativo europeo in merito all'utilizzo di intelligenza artificiale (IA in Italiano, *AI* nella lingua ufficiale dell'UE): il recentissimo Regolamento si pone come obiettivi il miglioramento del funzionamento del mercato e l'adozione di un'intelligenza artificiale affidabile e incentrata sull'uomo, garantendo, nel contempo, un elevato livello di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dell'UE (tra i quali eminentemente rilevante in questo contesto la protezione dei dati personali).

***AI Act*: obiettivi e ambito di applicazione**

Nel marzo di quest'anno il Parlamento Europeo ha approvato il Regolamento sull'intelligenza artificiale (c.d. *AI Act*), il cui obiettivo è "*proteggere i diritti fondamentali, la democrazia, lo Stato di diritto e la sostenibilità ambientale dai sistemi di IA ad alto rischio, promuovendo nel contempo l'innovazione e assicurando all'Europa un ruolo guida nel settore*", stabilendo obblighi per i fornitori e gli utilizzatori di intelligenza artificiale con un approccio basato sul rischio e sulla valutazione di impatto delle sue conseguenze.

Il Regolamento, recentemente approvato dal Consiglio, entra in vigore 20 giorni dopo la pubblicazione in Gazzetta Ufficiale dell'UE e diventa direttamente applicabile 24 mesi dopo la stessa, con prescrizioni e scadenze progressive (anche oltre i 24 mesi di cui sopra). Il Regolamento, che d'ora in poi chiameremo per semplicità *AI Act*:

- stabilisce regole armonizzate per l'immissione sul mercato, la messa in servizio e l'uso dei sistemi di intelligenza artificiale (sistemi di IA) all'interno dell'UE;
- prevede il divieto di determinate pratiche ed elenca i requisiti specifici per i sistemi di IA "*ad alto rischio*";
- stabilisce le regole di trasparenza per i sistemi di IA destinati a interagire con le persone fisiche e le regole in materia di monitoraggio e vigilanza del mercato.

L'*AI Act* si applica ai fornitori che immettono sul mercato o mettono in servizio sistemi di IA nell'Unione Europea, nonché agli utilizzatori (*deployer*[1]) di questi sistemi e a tutti i soggetti

(produttori o utilizzatori) extraUE che producano *output* utilizzati nel territorio della stessa.

Perimetrazione dei sistemi di IA e dei relativi rischi

Approcciamo la lettura del disposto normativo, quindi, con lo sguardo dell'utilizzatore (*deployer*) o del produttore di un sistema di IA che interagisce con quella particolare e ben identificata categoria di soggetti individuata dalla normativa italiana quale quella dei "*lavoratori*", precisando che la definizione di lavoratore è intesa dall'autrice nell'accezione dell'articolo 2, D.Lgs. 81/2008, e cioè non strettamente connessa al lavoro subordinato, ma a tutte le posizioni che espongono un soggetto umano allo "*svolgimento di un'attività lavorativa nell'ambito dell'organizzazione di un datore di lavoro pubblico o privato, con o senza retribuzione, anche al solo fine di apprendere un mestiere, un'arte o una professione*".

Ma che cos'è, davvero, un sistema di intelligenza artificiale?

Nel testo del Regolamento, all'articolo 3, troviamo la definizione sulla quale costruire i nostri ragionamenti: per "*sistema di intelligenza artificiale*" o "*sistema di IA*" si intende "*un software sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I*[2]*, 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*".

Ciò significa, e non è assolutamente trascurabile, che un sistema di intelligenza artificiale è certamente un *software*, ma diverso dai gestionali cui siamo abituati, perché "*apprende o ha appreso*" dalle moli di dati che gli sono (o sono state) sottoposte e che produce, sulla base di tecniche di inferenza statistica, contenuti, previsioni, raccomandazioni o decisioni che influenzano, nel nostro caso, il rapporto di lavoro.

Espone quindi matematicamente alla decisione automatizzata?

La risposta tecnica è no (non necessariamente), la risposta sensata, invece, è sì, perché un sistema di questo tipo esclude a priori tutto ciò che non conosce o non ha appreso e può, quindi, anche se non è l'attore della decisione, influenzare significativamente il comportamento dell'umano che la prende.

L'autrice rileva quindi, *in primis*, che l'utilizzo di un sistema di intelligenza artificiale nel contesto della gestione delle risorse umane può implicare la sussistenza di una decisione automatizzata e, quindi, tutte le obbligazioni già vigenti (in Italia e in UE) in materia di trasparenza nei confronti dei lavoratori e del relativo esercizio dei diritti di libertà previsti dal GDPR (Regolamento UE 2016/679, con particolare attenzione alle prescrizioni dell'articolo 22).

In secundis, l'autrice rileva che il Legislatore europeo ha adottato, come in tutta la normativa rilevante in materia, un approccio basato sul rischio e su questo ha fondato l'intero impianto

normativo. L'intelligenza artificiale presenta, infatti, accanto a molti benefici, la possibilità di essere utilizzata impropriamente e di fornire strumenti nuovi e potenti per pratiche di manipolazione, sfruttamento e controllo sociale, particolarmente dannose e contradditorie dei relativi diritti al rispetto della dignità umana, della libertà, dell'uguaglianza, della democrazia, della non discriminazione, della protezione dei dati e della vita privata, oltre che, evidentemente, dello Stato di diritto.

È proprio l'adozione dell'approccio basato sul rischio che ha indotto il Legislatore a effettuare una prima classificazione dei sistemi di intelligenza artificiale e a individuare 3 macro categorie di sistemi:

1. quelli vietati perché eccessivamente rischiosi;
2. quelli ad alto rischio (tra i quali compaiono quelli relativi alle risorse umane), che possono essere prodotti e utilizzati con opportune misure mitigazione del rischio;
3. quelli a rischio minimo.

Considerando che i sistemi di IA affidabili dovrebbero essere responsabili, concepiti per tutti (tenendo conto, nella loro progettazione, degli individui vulnerabili ed emarginati), non discriminatori, sicuri e trasparenti e rispettare l'autonomia umana e i diritti fondamentali, il regolatore valuta quindi:

- non utilizzabili: i sistemi di IA che determinano un rischio inaccettabile per la sicurezza, i mezzi di sussistenza e i diritti delle persone, perché consentono di manipolare il comportamento umano (compreso il *social scoring* che ha rilevanza anche in ambito di lavoro, come sostenuto da recenti sentenze di Corti italiane in materia di utilizzo dei sistemi di profilazione per l'attribuzione degli incarichi ai lavoratori addetti alla consegna a domicilio). Tra questi risultano particolarmente rilevanti nel contesto tutti gli eventuali sistemi di riconoscimento facciale e delle emozioni utilizzati sul luogo di lavoro, eccetto che per motivi medici o di sicurezza (ad esempio, il monitoraggio dei livelli di stanchezza di un pilota).
- ad alto rischio: sistemi di IA che possono potenzialmente avere ripercussioni negative sulla sicurezza delle persone o sui loro diritti fondamentali, tra i quali rientrano a pieno titolo la gran parte dei sistemi di intelligenza artificiale relativi alla gestione delle risorse umane: dal testo dell'*AI Act* (cons 57) si evince, infatti, che *"anche i sistemi di IA utilizzati nel settore dell'occupazione, nella gestione dei lavoratori e nell'accesso al lavoro autonomo, in particolare per l'assunzione e la selezione delle persone, per l'adozione di decisioni in materia di promozione e cessazione del rapporto di lavoro, nonché per l'assegnazione dei compiti, 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 future prospettive di carriera e sostentamento. [...] I sistemi di IA utilizzati per monitorare le prestazioni e il comportamento di tali persone possono inoltre incidere sui loro diritti in materia di protezione dei dati e vita privata";*
- a rischio minimo: che non implicano significativi rischi per i diritti e libertà delle

persone fisiche (e non impattano in alcun modo la gestione delle risorse umane, *ndA*).

Sintesi delle regole per i sistemi di IA ad alto rischio e concernenti le risorse umane

Se nella norma esiste una distinzione tra i sistemi a basso e alto rischio – per la salute e la sicurezza e per i diritti fondamentali degli individui – la stessa implica che tutti (o quasi) i sistemi utilizzabili in ambito lavorativo siano classificati come ad alto rischio. Di qui una serie di regole specifiche di trasparenza, sorveglianza umana, informazione individuale e collettiva, prima di mettere in opera o utilizzare un sistema di IA.

In breve, le prescrizioni dell'*AI Act* per i sistemi ad alto rischio prevedono che:

1. un sistema di IA ad alto rischio possa essere immesso o messo a disposizione degli utilizzatori sul mercato dell'Unione Europea solo dietro una valutazione di conformità per un IA affidabile (e.g. qualità dei dati, tracciabilità, trasparenza, sorveglianza umana, accuratezza, *cybersecurity*, etc.);
2. un sistema di IA ad alto rischio debba essere tecnicamente robusto, per garantire che la tecnologia sia adatta allo scopo e che i risultati falsi (positivi o negativi) non incidano in modo sproporzionato sui soggetti protetti (e.g. categorie di lavoratori, livello, CV, etnia, genere, età, etc.);
3. un sistema di IA ad alto rischio debba essere stato addestrato e testato con *set* di dati sufficientemente rappresentativi per ridurre al minimo il rischio di integrare distorsioni inique nel modello e garantire che, se presenti, queste possano essere risolte mediante opportune misure di rilevazione, correzione e attenuazione;
4. l'utilizzo di un sistema di IA ad alto rischio sia suffragato da una valutazione d'impatto sui diritti fondamentali (prodotta a cura del fornitore e recepita dal *deployer*, *ndA*).

Certamente quindi, in capo ai fornitori di tecnologia e sistemi di intelligenza artificiale nella gestione del personale, compresi i controlli a distanza, vigono tutte le regole sancite dall'*AI Act* e, in particolare, quelle dell'articolo 9 relative al sistema di gestione dei rischi, che prevedono che:

- sia istituito, attuato, documentato e mantenuto un sistema di gestione dei rischi;
- esso consista in un processo iterativo continuo eseguito nel corso dell'intero ciclo di vita del sistema e che preveda l'individuazione e analisi dei rischi associati al sistema di IA e di quelli correlati;
- siano adottate adeguate misure di mitigazione dei rischi individuati.

Se, però, il problema pare tutto in carico ai fornitori, in realtà non esime gli utilizzatori (o per meglio dire i *deployer*, cioè le organizzazioni, pubbliche o private, utilizzatrici del *software*) dall'acquisizione di documentazione e informazioni che suffraghino quanto sopra e, quindi, dimostrino la conformità (proprio perché i soggetti passivi dell'applicazione del Regolamento

non sono solo i produttori dei sistemi di intelligenza artificiale, ma anche i relativi utilizzatori).

AI Act e GDPR: decisione automatizzata e trasparenza

In questo contesto l'*AI Act* non esclude, bensì rafforza, qualora fosse necessario ribadirlo, l'obbligo imposto dal GDPR (Regolamento UE 2016/679) ai titolari del trattamento (nel nostro caso i datori di lavoro) di verificare, da parte dei fornitori, l'adozione e il mantenimento di misure adeguate per la protezione dei dati personali (si veda, in particolare, il testo dell'articolo 28, Regolamento UE 2016/679), nella fattispecie dei lavoratori, onde evitare danni non solo alla riservatezza, ma anche all'integrità e alla disponibilità di informazioni rilevanti e necessarie per la gestione del rapporto di lavoro nel contesto giuslavoristico del singolo Stato membro.

Inoltre, nulla togliendo alle già vigenti prescrizioni in materia di trasparenza nei confronti dei lavoratori, l'*AI Act* precisa nel suo testo alcune disposizioni normative estremamente rilevanti in ambito datoriale per comprendere le modalità di applicazione dei sistemi di intelligenza artificiale nel rapporto di lavoro. Il considerando 72 recita, infatti:

"*Per rispondere alle preoccupazioni relative all'opacità e alla complessità di determinati sistemi di IA e aiutare i deployer ad adempiere ai loro obblighi a norma del presente regolamento, è opportuno imporre la trasparenza per i sistemi di IA ad alto rischio prima che siano immessi sul mercato o messi in servizio. I sistemi di IA ad alto rischio dovrebbero essere progettati in modo da consentire ai deployer di comprendere il funzionamento del sistema di IA, valutarne la funzionalità e comprenderne i punti di forza e i limiti. I sistemi di IA ad alto rischio dovrebbero essere accompagnati da informazioni adeguate sotto forma di istruzioni per l'uso. Tali informazioni dovrebbero includere le caratteristiche, le capacità e i limiti delle prestazioni del sistema di IA. Tali elementi comprenderebbero informazioni su possibili circostanze note e prevedibili connesse all'uso del sistema di IA ad alto rischio, compresa l'azione del deployer suscettibile di influenzare il comportamento e le prestazioni del sistema, nel quadro dei quali il sistema di IA può comportare rischi per la salute, la sicurezza e i diritti fondamentali, sulle modifiche che sono state predeterminate e valutate a fini di conformità dal fornitore e sulle pertinenti misure di sorveglianza umana, comprese le misure volte a facilitare l'interpretazione degli output del sistema di IA da parte dei deployer. La trasparenza, comprese le istruzioni per l'uso che la accompagnano, dovrebbe aiutare i deployer a utilizzare il sistema e a prendere decisioni informate. Tra l'altro, i deployer dovrebbero essere nella posizione migliore per effettuare la scelta corretta del sistema che intendono utilizzare alla luce degli obblighi loro applicabili, essere a conoscenza degli usi previsti e vietati e utilizzare il sistema di IA in modo corretto e opportuno*".

Poche *chance* si intravedono, quindi, dal punto di vista dei datori di lavoro, per la possibilità di attribuire al fornitore la responsabilità di aver progettato un sistema di IA non sicuro.

Il testo del Regolamento è chiaro nell'attribuire all'utilizzatore (*deployer*) del *software* la

responsabilità nella scelta dell'utilizzo del prodotto, della sua configurazione nel contesto aziendale e anche della sorveglianza umana.

Della gestione automatizzata (con o senza intelligenza artificiale) dei rapporti di lavoro si è occupato anche il Legislatore italiano, che all'articolo 1-*bis*, D.Lgs. 152/1997, ha previsto che il datore di lavoro debba "*informare il lavoratore dell'utilizzo di sistemi decisionali o di monitoraggio integralmente automatizzati deputati a fornire indicazioni rilevanti ai fini dell'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*".

In aggiunta alle prescrizioni dello Statuto dei Lavoratori (L. 300/1970), quindi, l'attuale normativa nazionale (prima dell'*AI Act*) prevedeva la comunicazione delle informazioni relative ai sistemi informativi capaci di adottare una decisione automatizzata e, quindi, influenzare significativamente il rapporto di lavoro, non solo ai lavoratori, in occasione della costituzione del rapporto e ad ogni cambiamento dello stesso, bensì anche alle rappresentanze sindacali individuate da ogni organizzazione in funzione del proprio assetto.

Alle prescrizioni già esistenti si aggiungono, quindi, le nuove previsioni dell'*AI Act*, dettate dall'articolo 13, che prevedono che siano fornite trasparenti informazioni agli utilizzatori e, in particolare, che i sistemi di IA ad alto rischio (tra i quali quelli in ambito di lavoro):

- siano progettati e sviluppati in modo tale da garantire che il loro funzionamento sia sufficientemente trasparente da consentire agli utilizzatori (datori di lavoro, *deployer*) di interpretare l'*output* del sistema e utilizzarlo adeguatamente;
- siano accompagnati da istruzioni per l'uso in un formato digitale o non digitale appropriato, comprendendo informazioni concise, complete, corrette e chiare, pertinenti, accessibili e comprensibili per gli utilizzatori (*deployer*).

AI Act e GDPR: sorveglianza umana per i sistemi ad alto rischio concernenti le risorse umane

Onde, appunto, evitare gli elevati rischi per i diritti e le libertà delle persone (e nella fattispecie dei lavoratori) derivanti dall'applicazione di algoritmi di intelligenza artificiale al contesto di lavoro e limitanti, quindi, dello spazio di azione individuale e personale, l'*AI Act* prevede alcune rassicurazioni, eticamente comprensibili ma estremamente difficili da applicare nella gestione di un *software*, che concernono la sorveglianza umana delle decisioni prese o suggerite dall'algoritmo, e in particolare:

- che i sistemi di IA ad alto rischio siano progettati e sviluppati anche con strumenti di interfaccia uomo-macchina adeguati, in modo tale da poter essere efficacemente supervisionati da individui durante il periodo in cui il sistema di IA è in uso;
- che siano previsti un processo e un sistema di sorveglianza umana che mirino a

prevenire o ridurre al minimo i rischi per la salute, la sicurezza o i diritti fondamentali delle persone che possono emergere quando il sistema di IA è legittimamente utilizzato.

Quali quindi le cautele adottare nel rapporto di lavoro, nell'utilizzo di sistemi di IA?

La materia richiede l'applicazione e la declinazione di diverse norme e difficilmente si può ricondurre a un unico *corpus* regolatorio.

L'autrice si augura, però, che lettori e lettrici possano ritrovare nel testo gli spunti necessari per comprendere quali cautele adottare nel singolo contesto, partendo dall'assunto (non trascurabile) del fatto che ogni organizzazione economica è fatta a suo modo e richiede un'analisi specifica.

Nel nostro sistema nazionale, infatti, i più celebri o diffusi problemi emersi in sede giudiziaria sono stati originati dall'uso di algoritmi (di intelligenza artificiale o non) nel rapporto di lavoro e nei casi di controllo a distanza dei lavoratori non rispettosi del dettato della L. 300/1970, o in quelli di lavoro prestato tramite piattaforma digitale quali *riders*, ciclofattorini, corrieri di consegne a domicilio.

Nella maggior parte di questi contesti, prescindendo completamente dall'utilizzo di sistemi di intelligenza artificiale che apprendano dalle informazioni aziendali e/o dal comportamento dei lavoratori, le Autorità giudiziarie hanno sentenziato la prevalenza del diritto dei lavoratori di fronte ai meccanismi opachi, se non addirittura occulti, degli strumenti di decisione automatizzata e la necessità di rispetto non solo delle regole stabilite dall'articolo 4, L. 300/1970, ma anche della necessità di trasparenza assoluta (anche in sede sindacale) sul funzionamento (e, si badi bene, non sulla *disclosure* del codice o di alcuna forma di proprietà intellettuale, commerciale o tecnologica del datore di lavoro) degli algoritmi di *scoring*, valutazione e, quindi, decisione.

Volendo affrontare la tematica nel contesto della singola organizzazione, quindi, è necessario tenere conto non solo della regolamentazione lavoristica (compresi i dettati dei Ccnl), ma anche di alcune norme gerarchicamente più rilevanti, quali quelle sulla protezione dei dati personali e sull'utilizzo degli strumenti digitali, compresa l'intelligenza artificiale.

Per chi volesse vagliare l'ipotesi di implementare, assumendo il ruolo di *deployer*, un sistema di intelligenza artificiale applicato nel contesto del rapporto di lavoro, è necessario, quindi, occuparsi in maniera strutturata e sistemica di almeno:

- decisione consapevole (e documentazione della stessa) dell'utilizzo di sistemi informatizzati che implichino anche parzialmente la profilazione, la decisione automatizzata, l'uso di algoritmi di intelligenza artificiale per la gestione del rapporto

di lavoro in qualunque punto del suo ciclo di vita, dalla selezione fino alla cessazione, compresi i sistemi di controllo a distanza e di rilevazione delle presenze;
- esclusione a priori di dati personali non necessari o non pertinenti, con particolare attenzione ai dati biometrici, che necessitano di una specifica motivazione per l'utilizzo, qualunque il fondamento di liceità del trattamento dei dati personali adottato;
- analisi non sono funzionale, ma anche di sicurezza informatica e per la protezione dei dati, di ciascuno dei sistemi di cui sopra (comprese eventualmente le interfacce tra gli stessi);
- raccolta dal fornitore individuato (o in corso di selezione) di tutta la documentazione rilevante ai fini della valutazione della conformità alla vigente normativa e, quindi, la dimostrazione non solo della sicurezza e robustezza, ma anche della trasparenza e della possibilità di un intervento umano sul sistema e sul funzionamento degli algoritmi;
- documentazione e messa a disposizione di quanto sopra, in maniera trasparente, intelligibile e chiara, non solo ai lavoratori, ma anche alle organizzazioni sindacali pertinenti in funzione delle dimensioni dell'organizzazione.

Breve approfondimento sull'utilizzo di dati biometrici (con o senza sistemi di AI)

Se proprio qualcuno conservasse un ulteriore dubbio, l'autrice rassicura lettori e lettrici del fatto che non vi è alcuna correlazione automatica tra l'utilizzo di sistemi di IA e l'utilizzo di dati di natura biometrica.

L'utilizzo di dati "*biometrici*", secondo la definizione contenuta nel Regolamento UE 2016/679, all'articolo 4, è un utilizzo tecnologico di informazioni che individuano univocamente un soggetto umano, ma che non necessariamente prevedono l'utilizzo di algoritmi di intelligenza artificiale ("*dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici*").

Con moltissima probabilità, nella maggior parte dei casi (legittimi o meno), l'utilizzo corrente di dati biometrici dei lavoratori è effettuato per il tramite di *software* di mercato che sono in grado di rilevare l'informazione da un'immagine e confrontarla con un'altra informazione (come, per esempio, alcuni *scanner* utilizzati - illegittimamente - in epoca Covid allo scopo di rilevare la temperatura e consentire l'accesso alle sedi aziendali di grandi organizzazioni).

L'utilizzo di questa categoria di dati personali al fine dell'ordinaria gestione del rapporto di lavoro per garantire maggiore velocità e snellezza delle operazioni amministrative, come attestato diverse volte anche dall'Autorità garante per la protezione dei dati personali, non è conforme ai principi generali di minimizzazione e proporzionalità del trattamento.

In particolare, e prescindendo da qualunque sistema di IA che renderebbe la situazione ben più spinosa, l'autrice ricorda che il riconoscimento biometrico per controllare le attività e/o le presenze sul posto di lavoro viola la il diritto alla protezione dei dati dei lavoratori (si vedano in proposito i provvedimenti dell'Autorità garante per la protezione dei dati doc. web n. 9995680, 9995701, 9995741, 9995762, 9995785).

Risulta, quindi, evidente che il trattamento di dati biometrici nel contesto di lavoro è un'attività rischiosa, sia per il lavoratore sia per il datore di lavoro che non sia stato in grado di documentare la legittimità del trattamento. In questo, la combinazione di un sistema di rilevazione e gestione dei dati biometrici con un sistema di intelligenza artificiale non può che aggravare le circostanze: la sola ipotesi di combinare l'utilizzo di dati biometrici con sistemi di intelligenza artificiale attiverebbe un tale rischio nei confronti dei diritti e libertà dei soggetti sottoposti agli algoritmi, da concretizzarsi in una quasi matematica violazione sia dell'*AI Act* sia del GDPR, con tutte le conseguenze in termini di sanzioni, almeno amministrative, del caso.

[1] *AI Act, art 3, par 4): "deployer": una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un 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;*

[2] *L'allegato I declina, come approcci:*

a) Approcci di apprendimento automatico, compresi l'apprendimento supervisionato, l'apprendimento non supervisionato e l'apprendimento per rinforzo, con utilizzo di un'ampia gamma di metodi, tra cui l'apprendimento profondo (deep learning);

b) approcci basati sulla logica e approcci basati sulla conoscenza, compresi la rappresentazione della conoscenza, la programmazione induttiva (logica), le basi di conoscenze, i motori inferenziali e deduttivi, il ragionamento (simbolico) e i sistemi esperti;

c) approcci statistici, stima bayesiana, metodi di ricerca e ottimizzazione.