LABOR Il lavoro nel diritto

Pacini Giuridica

Il nuovo Regolamento sull'Intelligenza Artificiale ed il suo impatto sul mondo del lavoro

di A. Mariotti - *24 Ottobre 2024*

Introduzione

Il 12 luglio 2024 è stato pubblicato nella Gazzetta Ufficiale Europea il testo definitivo del Regolamento del Parlamento Europeo e del Consiglio n. 1689 del 13 giugno 2024, meglio conosciuto come AI Act.

L'impatto di questo nuovo Regolamento è ormai noto a tutti: è la prima fonte legislativa al mondo che disciplina (o che mira a disciplinare) a trecentosessanta gradi l'Intelligenza Artificiale, dallo sviluppo all'utilizzo finale, passando per i princìpi cardine ed arrivando in ultimo alle sanzioni nel caso di violazioni significative.

Il mondo del lavoro è sicuramente uno dei più coinvolti dalle novità introdotte dall'AI Act, poiché da tempo gran parte delle aziende utilizzano sistemi e *software* di Intelligenza Artificiale per ottimizzare la produttività, per gestire al meglio l'organizzazione del lavoro e, spesso, anche in fase precontrattuale per la valutazione dei candidati da assumere.

I datori di lavoro, che alla luce del nuovo Regolamento si identificano negli "utilizzatori" o, per meglio dire, nei "deployer" dei sistemi di AI, dovranno dunque adeguarsi alla nuova disciplina euro-unitaria, prevedendo catene di controllo molto stringenti e policy interne che descrivano i procedimenti di attuazione ed utilizzo delle "macchine intelligenti". Ma andiamo per gradi.

Alcune definizioni essenziali

All'interno dell'articolo 3 dell'AI Act si ritrovano alcune definizioni importanti, tra cui quella di "Intelligenza Artificiale" e di coloro che vi entrano in contatto durante il suo intero ciclo di vita.

L'Intelligenza Artificiale viene definita alla stregua di "*un sistema automatizzato progettato per funzionare con livelli di autonomia variabili 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*".

Rispetto alle prime Proposte di Regolamento, che cercavano di definire l'oggetto del suddetto atto tramite un rimando ad un allegato, oggi si assiste ad una definizione più concreta ed indipendente.

Nonostante ciò, la scelta del legislatore di prevedere più allegati al Regolamento in cui vengono elencate le diverse tipologie di AI non è casuale: questo permette di modificare più semplicemente la disciplina nel tempo, adeguandola alle nuove scoperte in ambito tecnologico e lasciando lo spazio per poterla ampliare, aggiungendo eventualmente altri allegati o modificando quelli attuali. Del resto, questa materia, più di altre, si presta ad un approccio dinamico per la rapidità con cui tali tecnologie si evolvono nel tempo.

Come chiarito dal Regolamento al Considerando n. 12, esulano dalla nozione di AI quei sistemi che "*utilizzano regole definite unicamente da persone fisiche per eseguire operazioni in modo automa- tico*". L'Intelligenza Artificiale non si riconosce dunque in *software* tradizionali o approcci di programmazione più semplici, ancorché integralmente automatizzati, che si basano su regole definite esclusivamente da persone fisiche per eseguire automaticamente operazioni: la caratteristica fondamentale dell'AI è la sua capacità inferenziale, che trascende l'elaborazione di base dei dati e consente l'apprendimento, il ragionamento o la modellizzazione. Ciò che contraddistingue strutturalmente un sistema intelligente è il grado di autonomia nella generazione degli output rispetto al coinvolgimento umano (S. Ciucciovino, *Risorse umane e intelligenza artificiale alla luce del regolamento (UE) 2024/1689, tra norme legali, etica e codici di condotta*, in *DRI*, 2024, 3, p. 574-575).

Per quanto riguarda invece i soggetti che interagiscono con l'AI, all'interno dell'art. 3 vengono fornite molte definizioni, tra cui quella di fornitore, di utente e di importatore. Il fornitore è: "*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*". Ecco, quindi, che viene identificato colui che è il "produttore" del sistema AI, che lo sviluppa e successivamente lo rivende o comunque lo mette a disposizione degli utenti interessati. È di fondamentale importanza riconoscere e identificare la figura del fornitore, poiché su di esso gravano i principali obblighi di trasparenza e di informazione rispetto ai sistemi AI da lui sviluppati ed immessi sul mercato.

La seconda figura che viene identificata è quella del deployer, ovvero: "*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*".

Il deployer è perciò colui che usufruisce direttamente del sistema AI, solitamente dopo averlo acquistato o comunque ottenuto dal fornitore.
Nel caso specifico, si pensi per esempio ad un datore di lavoro che, dopo aver acquistato un determinato software AI sul mercato, lo utilizzi all'interno della propria impresa per

controllare gli accessi al web del proprio personale, oppure acquisisca ed impieghi una tecnologia basata sull'AI che agevoli le mansioni più pesanti o pericolose in azienda, contribuendo al miglioramento delle condizioni di lavoro e di sicurezza. La definizione contenuta nell'AI Act specifica che, per essere definito "deployer", il soggetto utilizzatore deve applicare il sistema in un'attività professionale: per l'ambito applicativo di questo Regolamento non sono dunque considerati utenti tutti coloro che utilizzano software AI per attività strettamente personali (come, ad esempio, un'esperienza videoludica puramente ricreativa), che non incidono dunque sulla libertà o sui diritti fondamentali di soggetti terzi.

Infine, viene fornita anche una definizione di importatore, cioè: "*una persona fisica o giuridica ubicata o stabilita nell'Unione che immette sul mercato un sistema di IA recante il nome o il marchio di una persona fisica o giuridica stabilita in un paese terzo*". Per quanto riguarda infatti la normativa sull'AI, l'Europa, proprio con questo Regolamento, si può considerare all'avanguardia rispetto ad altre realtà come l'America o la Cina, in cui il diverso tipo di approccio tecnologico-culturale non garantisce tutte le tutele che qui sono previste.

Classificazione dei sistemi AI: l'approccio *risk-based*

L'impianto del Regolamento prevede il passaggio da una classificazione rigida di tipo *top-down* ad una più flessibile, in quanto soggetta a riesame permanente mediante una valutazione periodica e fondata sulla portata dell'impatto negativo che il sistema di AI determina sui diritti fondamentali protetti dalla Carta dell'UE. Tale classificazione è dunque impostata sulla valutazione del rischio (*risked-based*), ovvero dell'impatto più o meno forte che i sistemi di Intelligenza Artificiale possono avere sui soggetti interessati, comprese le relative conseguenze del loro utilizzo.
Sono quindi previsti tre diversi gruppi di sistemi AI, identificati secondo le loro caratteristiche principali e secondo il loro impatto: le "*pratiche di Intelligenza Artificiale vietate*", i "*sistemi di AI ad alto rischio*" ed infine, gli "*obblighi di trasparenza per determinati sistemi di AI*", ovvero quei sistemi cosiddetti a "basso rischio".

Applicazioni di Intelligenza Artificiale non ammesse

I sistemi di AI previsti all'art. 5 AI Act non possono essere utilizzati o immessi sul mercato. In particolare, è vietato l'utilizzo di quei sistemi AI:

1. di categorizzazione biometrica basati su caratteristiche sensibili;

2. di creazione di banche dati di riconoscimento facciale;

3. di riconoscimento delle emozioni sul luogo di lavoro, fatto salvo l'utilizzo di tale sistema per motivi medici o di sicurezza;

4. di manipolazione del comportamento umano o che sfruttano le vulnerabilità degli individui;

5. di valutazione o classificazione delle persone fisiche: tale valutazione non può difatti comportare un trattamento pregiudizievole e sproporzionato nei confronti di determinati individui rispetto ad altri a causa del loro comportamento sociale, e tale trattamento non può avere ripercussioni in contesti sociali non collegati a quello in cui sono stati raccolti i dati.

Il divieto qui previsto è assoluto: i *deployer*, e dunque anche i datori di lavoro, devono assicurarsi di non utilizzare tali sistemi, prevendo una stretta ed efficace comunicazione con il proprio fornitore, così da seguire pedissequamente le istruzioni da lui fornite ed evitando di incappare in utilizzi errati o vietati.

Per quanto attiene a questa categoria, nella prospettiva lavoristica si segnala la particolare rilevanza del divieto di utilizzo di sistemi di riconoscimento delle emozioni sul posto di lavoro, ad eccezione di quelli che riconoscono il dolore o la fatica per motivi medici o di sicurezza (M. Peruzzi, *Intelligenza Artificiale e lavoro: l'impatto dell'AI Act nella ricostruzione del sistema regolativo UE di tutela*, in M. Biasi (a cura di), *Diritto del lavoro ed Intelligenza Artificiale*, Giuffrè Editore, 2024, p. 125; S. Marassi, *Intelligenza artificiale e sicurezza sul lavoro*, *ibidem*, p. 207 ss.).

Tali sistemi possono dunque essere utilizzati solo in determinati e specifici luoghi di lavoro, e solo per specifiche necessità volte alla tutela dei lavoratori e di tutti coloro che si interfacciano con essi.

Sistemi di AI ad alto rischio ed il loro utilizzo in azienda

Per quanto concerne il mondo del lavoro, ai sensi dell'Allegato III, punto 4 dell'AI Act, sono considerati sistemi AI ad alto rischio tutti quei *software* relativi all'occupazione, gestione dei lavoratori ed accesso al lavoro autonomo. Tutti i sistemi utilizzati all'interno del ciclo produttivo di un'azienda saranno dunque classificati come ad alto rischio, comportando la necessità per il datore di lavoro, o per meglio dire per il *deployer*, di adeguare i propri standard di sicurezza alle previsioni del Regolamento.

In particolare, vengono descritti i sistemi applicati al settore dell'occupazione rientranti nella categoria ad alto rischio, ovvero i sistemi di AI destinati ad essere utilizzati per decidere l'assunzione o la selezione di persone fisiche e l'AI destinata ad essere utilizzata per adottare decisioni in materia di promozione e cessazione dei rapporti contrattuali di lavoro, per l'assegnazione dei compiti e per il monitoraggio e la valutazione delle prestazioni e del comportamento delle persone nell'ambito di tali rapporti di lavoro.

Come si evince dal testo del Regolamento, non solo è l'intero processo lavorativo a rientrare in questa classificazione, ma anche la fase precontrattuale della ricerca e della selezione del personale. Questa scelta del legislatore europeo, che possiamo certamente definire una determinazione etica e di grande valore sociale, evidenzia come l'UE, di fronte all'invadenza e l'invasività di certe pratiche, si sforzi di garantire il massimo livello di trasparenza e conoscibilità nelle scelte datoriali, tutelando il più possibile il lavoratore, pure impedendo forme di

discriminazione, in questo caso più sofisticate di altre, in tutti quei processi che investono i cittadini ed influenzano la loro vita ed il loro futuro.

Come anticipato, il rischio alto si presume soltanto se il sistema AI presenta un rischio "significativo" di danno per la salute, la sicurezza o per i diritti fondamentali delle persone fisiche e se influenza materialmente il processo decisionale. Ciò significa che la classificazione dei sistemi impiegati nel mondo del lavoro, ed in particolare nell'ambito delle risorse umane, non è automatica, ma dipende nel concreto da come è configurato il sistema, da come esso si inserisce nel processo decisionale e dalla potenziale probabilità di arrecare un danno "significativo" ai diritti fondamentali dei lavoratori. La valutazione di tutto ciò spetta però al fornitore, che deve documentare le sue scelte prima dell'immissione del software sul mercato e classificare i sistemi AI al momento della registrazione nell'apposita banca dati dell'UE. Ne discende che l'individuazione della classe di rischio dei sistemi applicati in ambito lavorativo è affidata all'autovalutazione del fornitore, all'interno della preliminare valutazione del rischio.

Rispetto a tale classificazione, il datore di lavoro, nella sua veste di utilizzatore, è un soggetto passivo che prende atto della classificazione operata dal fornitore: spetta a quest'ultimo consegnare al deployer le informazioni tecniche necessarie a rendere sufficientemente trasparente il funzionamento dell'AI, al fine di metterlo in grado di interpretare l'output del sistema, utilizzarlo adeguatamente ed assolvere ai propri obblighi (S. Ciucciovino, op. cit., pp. 580-581).

È bene comunque ricordare sempre che l'art. 6 AI Act, con rimando all'Allegato III, definisce in modo tassativo i sistemi ad alto rischio: la valutazione del fornitore non potrà mai superare le disposizioni ivi previste, ma anzi queste devono fungere da spartiacque per una garanzia di maggior sicurezza e certezza anche nei confronti dell'utilizzatore finale.

Responsabilità e catena di controllo

L'approccio cosiddetto "*risk-based"* si articola su tre livelli, ovvero: la valutazione e gestione del rischio, composta dalle fasi di identificazione, valutazione e mitigazione; un secondo livello che riguarda la gestione della qualità del sistema e, infine, la valutazione di conformità, basata anche sulla verifica della gestione della qualità precedentemente effettuata.

Questo modello fa sì che gli obblighi di garanzia, rispetto al funzionamento ed all'accettabilità dei rischi, gravino maggiormente in capo al fornitore del sistema e non sull'utilizzatore. Questo è uno dei motivi principali per cui l'AI Act è stato fortemente osteggiato dalle grandi Big-Tech produttrici di sistemi AI: con l'approvazione del Regolamento, l'immissione sul mercato europeo delle loro tecnologie viene subordinato al rispetto dell'iter di gestione dei rischi, che fino ad oggi non prevedeva nessun onere dettagliato, ma solo il rispetto generico dei princìpi generali dell'Unione e dei diritti fondamentali dell'uomo.

Il datore di lavoro non è però esente da responsabilità: il deployer, infatti, deve adottare idonee misure tecniche ed organizzative al fine di garantire un utilizzo dei sistemi AI ad alto rischio

conforme alle istruzioni per l'uso che accompagnano tali sistemi, redatte dai fornitori, in modo da evitare errori operativi che possano compromettere la sicurezza o i diritti fondamentali degli interessati.

In particolare, ai sensi dell'art. 26 AI Act, nella misura in cui esercita il controllo sui dati di input, il deployer deve garantire che tali dati siano pertinenti e sufficientemente rappresentativi per le finalità previste dal sistema di AI. Inoltre, il datore di lavoro deve monitorare costantemente il funzionamento del sistema, sulla base delle istruzioni per l'uso. Qualora abbia motivo di ritenere che l'uso del sistema AI possa comportare un rischio, deve informare tempestivamente il fornitore e la pertinente autorità di vigilanza del mercato, oltre a sospendere l'uso di tale sistema nel caso in cui si verifichi un incidente grave.

Si può dunque concludere che il datore di lavoro è titolare di una sorta di generale "corresponsabilità" insieme al fornitore, così che coloro che sono interessati dal trattamento effettuato dal sistema di Intelligenza Artificiale possono essere tutelati a partire dallo sviluppo e creazione del sistema stesso, fino all'utilizzo finale messo in atto dal deployer, che non solo deve sottostare alle istruzioni del fornitore, ma deve svolgere una vigilanza attiva ed un continuo monitoraggio sul funzionamento delle macchine.

Per fare ciò, le aziende devono assegnare la supervisione dei sistemi AI a persone fisiche che abbiano la formazione, le competenze e l'autorità necessarie per svolgere tale funzione. Difatti, ai sensi dell'art. 14 AI Act, i sistemi ad alto rischio devono essere progettati e sviluppati in modo tale da poter essere efficacemente supervisionati da persone fisiche durante il periodo in cui sono in uso. Le misure di sorveglianza, commisurate ai rischi, sono si individuate e garantite da parte del fornitore, prima dell'immissione sul mercato o della messa in servizio del sistema ad alto rischio, ma devono essere adatte per l'attuazione delle stesse da parte del deployer, ovvero il datore di lavoro.

Ciò significa che una volta ricevute le istruzioni dettagliate e comprensibili, il datore di lavoro può (o meglio, deve) delegare a dei responsabili capaci e competenti la sorveglianza riguardo all'utilizzo dei sistemi AI, tramite le indicazioni fornite.

Non solo: coloro che ricoprono questo ruolo devono essere in grado di monitorare debitamente il funzionamento dei software, anche al fine di individuare ed affrontare anomalie, disfunzioni e prestazioni inattese, alla luce delle previsioni dell'art. 26. Inoltre, essi devono essere in grado di saper scegliere, in qualsiasi situazione particolare, di non usare il sistema AI ad alto rischio o di ignorare, annullare o ribaltare l'output fornito dal sistema. Infine, devono potere essere in grado di intervenire sul funzionamento del sistema o di interrompere tale sistema mediante un pulsante di "arresto" o una procedura analoga.

Alla luce dei doveri sopra elencati, sempre più aziende si stanno dotando di apposite policy interne riguardo all'Intelligenza Artificiale, al fine di disciplinare, per lo meno internamente, tutto l'iter di valutazioni e controlli dei software utilizzati.

Formazione dei lavoratori

Per perseguire le indicazioni della nuova disciplina comunitaria, le aziende dovranno impegnarsi per garantire ai propri dipendenti un'adeguata formazione sull'utilizzo dei sistemi AI in uso all'interno delle loro organizzazioni. L'utilizzo di detti sistemi dovrà essere messo in atto in modo responsabile ed efficace non solo da coloro che saranno designati alla gestione dei software, ma da chiunque si interfaccerà con l'AI. Ogni possibile uso dovrà, comunque, essere necessariamente in linea con quanto previsto dalle istruzioni garantite dal fornitore del sistema AI.

L'aggiornamento dei dipendenti deve essere costante, poiché l'Intelligenza Artificiale si evolve giorno dopo giorno: un sistema che fino ad un anno fa era ritenuto innovativo, oggi potrebbe già essere desueto. È necessaria, dunque, una continua informazione in merito ai progressi dei sistemi AI, anche con riguardo alle potenziali preoccupazioni etiche che potrebbero avere un impatto sulla azienda e sullo svolgimento delle attività lavorative.

Questa nuova attività formativa sarà presumibilmente delegata a coloro che saranno i responsabili dei controlli sui sistemi AI, i quali, con il supporto del dipartimento IT interno ad ogni azienda, saranno i referenti delle iniziative di sensibilizzazione e formazione, da definire ed implementare in collaborazione con gli altri dipartimenti, sempre sotto il controllo del datore di lavoro.

Sanzioni: la cornice edittale europea in attesa della disciplina nazionale *ad hoc*

Per quanto riguarda il regime sanzionatorio, l'art. 99 dell'AI Act dispone che gli Stati membri debbano stabilire, al più tardi entro la data di entrata in applicazione del Regolamento, le norme relative alle sanzioni ed alle altre misure di esecuzione, che possono includere anche avvertimenti e misure non pecuniarie, applicabili in caso di violazione del Regolamento da parte degli operatori.

In attesa dunque di più specifiche indicazioni a livello nazionale, la cornice edittale prevista dal Regolamento prevede tre diverse fattispecie sanzionatorie:

1. La non conformità al divieto delle pratiche AI non ammesse, di cui all'art. 5, è soggetta a sanzioni amministrative pecuniarie fino ad euro 35.000.000 o, se l'autore del reato è un'impresa, fino al 7% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

2. La non conformità alle seguenti disposizioni, diverse da quelle di cui all'art. 5, è soggetta a sanzioni amministrative pecuniarie fino ad euro 15.000.000 o, se l'autore del reato è un'impresa, fino al 3% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

3. La fornitura di informazioni inesatte, incomplete o fuorvianti agli organismi notificati o alle autorità nazionali competenti per dare seguito a una richiesta è soggetta a sanzioni

amministrative pecuniarie fino ad euro 7.500.000 o, se l'autore del reato è un'impresa, fino all'1% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

In particolare, all'interno della fattispecie di cui al punto 2 vi rientrano tutti gli obblighi riservati al deployer, di cui all'art. 26, e gli obblighi di trasparenza di cui all'art. 50.

Il datore di lavoro dovrà perciò essere preciso e puntuale nell'adottare misure tecniche ed organizzative idonee ad un utilizzo conforme dei sistemi AI in base alle indicazioni del fornitore, attuare l'adeguata sorveglianza umana o affidarla a professionisti di cui comunque rimane responsabile, esercitare il controllo sui dati di input ed output, monitorare il funzionamento del sistema durante il suo intero ciclo di vita ed informare i lavoratori interessati, oltre ai loro rappresentanti, in merito all'utilizzo del sistema ad alto rischio ed alla sua invasività. In particolare, per quanto riguarda la normativa italiana, nel caso in cui il datore di lavoro non ottemperasse al suo dovere di informazione nei confronti dei rappresentanti dei lavoratori, potrebbe certamente configurarsi una condotta antisindacale ai sensi dell'art. 28 dello Statuto dei Lavoratori, con il conseguente rischio di incorrere anche in sanzioni penali.

Come evidenziato dunque, le sanzioni per il mancato adempimento dei suddetti oneri da parte del deployer sono molto consistenti: l'intento del Regolamento è chiaramente dissuasivo, al fine di evitare incidenti o utilizzi sbagliati di sistemi altamente avanzati, che potrebbero comportare forti discriminazioni soprattutto in ambito lavorativo ed in quello della ricerca e selezione del personale. Difatti, anche se la crescente applicazione di sistemi automatizzati promette di neutralizzare il margine di discrezionalità o errore umano, numerosi studi hanno dimostrato che persino le tecnologie algoritmiche più sofisticate non sono immuni al pregiudizio ed alla discriminazione (P. De Petris, *La discriminazione algoritmica. Presupposti e rimedi*, in *Diritto del lavoro ed Intelligenza Artificiale*, in M. Biasi (a cura di), Diritto del lavoro e intelligenza artificiale, cit., p. 225-226).

Conclusioni

Dalla nuova disciplina comunitaria emerge la volontà dell'Unione Europea di fissare degli standard di informazione e sicurezza in merito all'utilizzo di tutti i sistemi che hanno visto la luce grazie allo sviluppo dell'Intelligenza Artificiale.

Le aziende, direttamente coinvolte in questo nuovo vortice innovativo, dovranno dimostrare di saper stare al passo della nuova tecnologia, coinvolgendo i lavoratori per farli sentire parte integrante del cambiamento: l'AI è uno strumento molto potente che, se impiegato in modo ottimale, potrà portare grandi benefici ad entrambe le parti coinvolte nel rapporto di lavoro.

Un'ulteriore sfida attende anche le relazioni industriali, ben potendo oggi le soluzioni contrattuali-collettive anticipare il cambiamento tecnologico, senza subirlo passivamente com'è stato fino ad ora (M. Biasi, *Il lavoro nel d.d.l. governativo in materia di intelligenza artificiale: principi, regole, parole, silenzi*, in *DRI*, 2024, 3). La grande flessibilità potenziale della contrattazione a livello collettivo può portare a proporre soluzioni duttili e adattabili ai singoli

contesti produttivi, adeguando così il panorama normativo italiano alle crescenti necessità di innovazione e tutela imposte dall'Unione Europea.

Alessandro Mariotti, praticante avvocato in Milano

Visualizza il documento: Regolamento UE del Parlamento Europeo e del Consiglio 13 giugno 2024 2024, n. 1689