RESPONSABILITÀ DATORIALI NELL'IMPIEGO DEGLI STRUMENTI DI IA: TRA INNOVAZIONE E INCERTEZZE NORMATIVE

Marcello Deotto*

Il presente contributo si prefigge di analizzare le responsabilità del datore di lavoro nell'impiego di strumenti di intelligenza artificiale, evidenziando le implicazioni normative introdotte dall'"AI Act" e il loro impatto sul diritto del lavoro. L'analisi si concentra sul contrasto tra l'approccio europeo, che attribuisce un ruolo centrale ai fornitori di IA, e il quadro giuslavoristico nazionale, che invece impone al datore di lavoro obblighi di gestione e tutela dei lavoratori.
Dopo un inquadramento normativo delle diverse figure in campo e dei loro rispettivi obblighi, si esamineranno le criticità legate all'opacità dei sistemi e alla difficoltà di attribuzione delle responsabilità. Successivamente, verranno esplorate le diverse soluzioni giuridiche, valutando sia la prospettiva giuslavoristica che quella civilistica.
L'approccio seguito combina analisi normativa, giurisprudenziale e teorica, al fine di offrire al lettore una panoramica delle sfide davanti alle quali ci troviamo e delle loro possibili soluzioni.
La riflessione si inserisce nel più ampio dibattito sulla regolamentazione dell'intelligenza artificiale nel contesto lavorativo, reso particolarmente attuale dalle recenti iniziative normative europee.
L'introduzione dell'"AI Act" a livello europeo ha infatti suscitato una vivace discussione su come gestire e orientare al meglio l'utilizzo di queste tecnologie negli ambienti di lavoro.
Tra le problematiche emerse particolarmente significativo è appunto la questione relativa al ruolo e alle responsabilità del datore di lavoro nell'utilizzo di strumenti di intelligenza artificiale.
Del resto, la complessità e l'opacità dei modelli di IA rendono difficile identificare le cause specifiche di un danno e di conseguenza, determinare i soggetti chiamati a rispondere per la condotta del sistema.
Al fine di ovviare a questa problematica, la normativa distingue i piani di responsabilità suddividendola tra il "provider"[1] (chi sviluppa e immette sul mercato il sistema di IA) e il "deployer" (chi utilizza il sistema, ovvero il datore di lavoro)[2].
I "providers" hanno la responsabilità primaria di garantire che i sistemi siano conformi ai requisiti stabiliti dall'"AI Act", assicurandone il rispetto degli standard di sicurezza, trasparenza e affidabilità individuati dal regolamento (art. 16). Tra gli obblighi a questi attribuiti rientrano l'analisi dei rischi associati ai sistemi di intelligenza artificiale (art. 9), la conservazione e tracciabilità dei dati utilizzati e delle operazioni svolte (art. 12), il rispetto delle garanzie di trasparenza e di informazione sul funzionamento del sistema (art. 13). Inoltre, i "providers" devono garantire che i loro sistemi siano progettati in modo da consentire una supervisione umana efficace, prevenendo risultati indesiderati o dannosi (art. 14), monitorando continuamente i sistemi immessi sul mercato e adottando eventuali misure correttive in caso di criticità emergenti (art. 17). La conformità normativa è garantita anche

* Dottorando di ricerca in Diritto, mercato e persona presso l'Università Ca' Foscari di Venezia.
[1] «È "fornitore": 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, punto 3).
[2] «È "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» (art. 3 parag. 1 punto 4).

attraverso l'obbligo di predisporre una documentazione tecnica dettagliata (art. 11), che deve includere informazioni relative alla progettazione, alla logica dell'algoritmo, ai "dataset" utilizzati e ai meccanismi di mitigazione dei "bias". Inoltre, ai sensi dell'art. 75, i "providers" sono soggetti a controlli di conformità e certificazioni, soprattutto per i sistemi ad alto rischio, al fine di garantire che le tecnologie implementate rispettino i criteri imposti dal regolamento.

I "deployers" hanno invece responsabilità più limitate. Esse includono l'obbligo di verificare che il sistema venga utilizzato secondo le istruzioni fornite, la formazione adeguata del personale coinvolto (art. 26), il monitoraggio delle prestazioni (art. 29) e la segnalazione tempestiva al "provider" e alle autorità competenti di eventuali incidenti o malfunzionamenti significativi[3]. I "deployers" hanno inoltre il compito di provvedere alla conservazione per un periodo adeguato[4] dei "log" generati automaticamente, anche al fine di facilitare eventuali verifiche o indagini successive.

Il rapporto tra "provider" e "deployer" sembrerebbe quindi caratterizzato da una stretta interdipendenza e complementarietà tra le due figure, attribuendo però al "provider", i maggiori oneri in termini di verifica e organizzazione dell'impianto utilizzato, privilegiando una valutazione a monte dei possibili effetti distorsivi[5].

Le motivazioni che hanno portato il legislatore europeo ad adottare questa soluzione normativa devono essere ricondotte ad una complessità di ragioni, tra cui spiccano le specificità tecniche che contraddistinguono gli strumenti di intelligenza artificiale.

Infatti, come noto i modelli informatici di AI operano tramite un processo suddiviso in diverse fasi. Ad un momento inziale in cui vengono inserite nella macchina le informazioni da processare ("input"), segue la fase di rielaborazione, compiuta in autonomia dal sistema all'interno delle così dette "black box". L'attività di analisi e assemblaggio delle nozioni che caratterizza questo momento avviene sulla base delle indicazioni avute nel percorso di addestramento compiuto al momento della programmazione[6]. Una volta che i dati inseriti sono stati analizzati e trattati, il sistema giunge agli "output", ovvero i risultati che l'intero processo ha generato.

Se i dati inseriti in fase di avviamento possono essere ritenuti verosimilmente certi, al contempo risulta molto più difficile per lo stesso programmatore determinare come la macchina rielaborerà le indicazioni raccolte[7].

---

[3] Cfr. art. 26, par. 5, «I deployer monitorano il funzionamento del sistema di IA ad alto rischio sulla base delle istruzioni per l'uso e, se del caso, informano i fornitori a tale riguardo conformemente all'articolo 72. Qualora abbiano motivo di ritenere che l'uso del sistema di IA ad alto rischio in conformità delle istruzioni possa comportare che il sistema di IA presenti un rischio ai sensi dell'articolo 79, paragrafo 1, i deployer ne informano, senza indebito ritardo, il fornitore o il distributore e la pertinente autorità di vigilanza del mercato e sospendono l'uso di tale sistema. Qualora abbiano individuato un incidente grave, i deployer ne informano immediatamente anche il fornitore, in primo luogo, e successivamente l'importatore o il distributore e le pertinenti autorità di vigilanza del mercato. Nel caso in cui il deployer non sia in grado di raggiungere il fornitore, si applica *mutatis mutandis* l'articolo 73. Tale obbligo non riguarda i dati operativi sensibili dei deployer dei sistemi di IA che sono autorità di contrasto».

[4] Pari ad almeno sei mesi.

[5] Ciò anche alla luce di quanto espresso nel considerando 79 dell'"AI Act" secondo cui «È opportuno che una specifica persona fisica o giuridica, definita come il fornitore, si assuma la responsabilità dell'immissione sul mercato o della messa in servizio di un sistema di IA ad alto rischio, a prescindere dal fatto che tale persona fisica o giuridica sia la persona che ha progettato o sviluppato il sistema».

[6] S. Ciucciovino, *La disciplina nazionale sulla utilizzazione della intelligenza artificiale nel rapporto di lavoro*, in *Lavoro Diritti Europa* 1 (2024) 13-14.

[7] Non a caso si parla di "black box" per intendere le scatole nere o scatole oscure in cui queste informazioni vengono rielaborate e assemblate dal sistema medesimo.

L'opacità dei risultati predisposti dal sistema favorisce quindi l'emanazione di regole stringenti verso il fornitore del sistema, il quale ha il compito di insegnare alla macchina nella fase di addestramento i limiti attorno ai quali questa è chiamata ad operare.

Tale approccio, volto ad attribuire la responsabilità delle operazioni compiute in capo a chi ha ideato e fornito il sistema, si scontra però con l'impianto normativo che caratterizza il diritto del lavoro, il quale assegna al datore di lavoro le incombenze derivanti dalla conduzione dell'impresa.

Infatti, da un lato l'art. 2086 c.c., valorizzando la dimensione gerarchica che caratterizza ogni struttura aziendale, riconosce al datore di lavoro il ruolo di capo dell'impresa[8]. Dall'altro, ragionando in termini di salute e sicurezza, l'art. 2087 c.c., conferisce al datore di lavoro il compito di tutelare l'integrità fisica e la personalità morale dei prestatori di lavoro, tenuto conto della particolarità del lavoro, dell'esperienza e della tecnica.

Sulla base di queste considerazioni è quindi possibile rilevare un paradossale contrasto normativo tra la normativa europea, volta a privilegiare il ruolo del fornitore dei sistemi, e l'ordinamento giuslavoristico che attribuisce maggiori responsabilità in capo al datore di lavoro. A ciò si affianca il rischio di un basso grado di consapevolezza del datore davanti alle decisioni prese dai sistemi di intelligenza artificiale rispetto alle quali potrebbe essere chiamato a rispondere[9].

In primo luogo, è quindi fondamentale interrogarsi su come colmare la frattura normativa realizzatasi, analizzando i diversi profili di responsabilità che coinvolgono il datore di lavoro.

In un'ottica civilistica vi è chi ha valutato la responsabilità del datore per l'utilizzo di AI in relazione alla disciplina delle attività pericolose regolate dall'art. 2050 c.c.[10]. Questa ipotesi, apparentemente in linea con l'approccio "risk based" del regolamento, è stata recepita anche dal Parlamento Europeo nell'ambito della risoluzione del 20 ottobre 2020[11], il quale ha riconosciuto come l'utilizzatore dell'intelligenza artificiale realizza attraverso questo strumento un'attività pericolosa[12] e pertanto debba esse sottoposto ad un regime di responsabilità oggettiva. Tale argomentazione, isolatamente considerata, si presta però a critiche[13].

---

[8] In combinato disposto con l'art. 2104 c.c.

[9] Ciò vale anche in relazione all'art. 2087, rispetto al quale la Corte di cassazione ha più volte affermato come esso non configuri un'ipotesi di responsabilità oggettiva. Infatti, anche in riferimento alla salute e sicurezza, l'elemento essenziale resta la colpa, motivo per cui dalla norma non si può dedurre l'imposizione di un obbligo assoluto di adottare qualsiasi misura precauzionale possibile e non espressamente prevista, al fine di prevenire qualunque danno. Di conseguenza, la responsabilità del datore di lavoro non può essere considerata automatica ogniqualvolta si verifichi un danno, essendo invece necessario dimostrare come l'evento sia riconducibile a una sua colpa, derivante dalla violazione di obblighi imposti dalla legge o suggerito dalle migliori pratiche tecniche (Cass., Sez. IV, 23/05/2019, n. 14066, Cass., Sez. IV, 25/10/2021, n. 29909, Cass., Sez. IV, 29/01/2013, n. 2038, Cass., Sez. IV, 17/05/2013, n. 12089, Cass., Sez. IV, 12/07/2004, n. 12863, Cass., Sez. IV, 10/05/2000, n. 6018).

[10] S. Cairoli, *Intelligenza artificiale e sicurezza sul lavoro: uno sguardo oltre la siepe*, in *Diritto della Sicurezza sul Lavoro* 2 (2024) 35ss.

[11] European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)).

[12] Al punto 14 della risoluzione si riconosce che «il tipo di sistema di IA su cui l'operatore esercita il controllo è un fattore determinante con riferimento alla responsabilità; si osserva che un sistema di IA che comporta un rischio intrinseco elevato e che agisce in modo autonomo è potenzialmente molto più pericoloso per il pubblico; si ritiene che, sulla base delle sfide giuridiche che i sistemi di IA pongono per i regimi di responsabilità civile esistenti, appare ragionevole istituire un regime comune di responsabilità oggettiva per tali sistemi di IA autonomi ad alto rischio; si sottolinea che tale approccio basato sul rischio, che potrebbe comprendere diversi livelli di rischio, dovrebbe basarsi su criteri chiari e su una definizione adeguata di alto rischio e garantire la certezza giuridica».

[13] G.G. Crudeli, *Sistemi di intelligenza artificiale autonomi e responsabilità datoriale*, in *Diritto della Sicurezza sul Lavoro* 2 (2024) 421-422. Vedi anche G. D'Alfonso, *Intelligenza artificiale e responsabilità civile. Prospettive europee*,

L'assunto, ragionevolmente considerabile per i sistemi di intelligenza artificiale ad alto rischio, diversamente potrebbe trovare spazio per ogni sistema di AI utilizzato. In tal modo, si giungerebbe all'errata conclusione che i sistemi a rischio diverso da quello alto o da quello inaccettabile possano essere forieri di danni, argomentazione che difficilmente potrebbe essere accolta.

Alcuni autori hanno quindi provato a risolvere la dicotomia normativa riconducendo il problema all'art. 2048 c.c., ovvero ipotizzando che, come il genitore, viene chiamato a rispondere per i danni arrecati dal figlio, parallelamente l'addestratore debba essere l'unico chiamato a rispondere per i danni arrecati dal sistema di intelligenza artificiale che ha educato, realizzando una sorta di *culpa in educando* innovativa[14]. Anche tale ipotesi suscita qualche perplessità. Infatti, se accettassimo il parallelismo tra addestratore e genitore, si ricondurrebbe la causa del danno unicamente alla fase di addestramento, con ciò escludendo altre possibili ipotesi dannose che tuttavia potrebbero comunque emergere. Inoltre, accogliendo tale tesi, non si terrebbero adeguatamente in considerazione i vincoli derivanti dal rapporto di lavoro, volti a condizionare in un modo o nell'altro l'attività del datore. Del resto, ciò risulterebbe palesemente in contrasto con il dettame del regolamento che comunque affida all'utilizzatore importanti compiti di monitoraggio e valutazione dello strumento.

Diversamente si è provato a ragionare utilizzando lo strumento della responsabilità per padroni e committenti individuata dall'art. 2049 c.c. In questa prospettiva, il datore di lavoro, accetterebbe implicitamente il rischio potenziale derivante dall'aver affidato alla macchina determinate mansioni, al pari di un *procurator* o comunque di un delegato del datore, in un'ottica che è quella del rischio d'impresa che contraddistingue ogni attività imprenditoriale[15]. Questa impostazione determinerebbe una responsabilità del datore di lavoro che sarebbe chiamato a rispondere oggettivamente per i danni arrecati dalla macchina quale *culpa in eligendo*[16].

---

in *Revista de Estudios Juridicos y Criminologicos* 6 (2022) 173 per cui «l'intelligenza artificiale non è intrinsecamente pericolosa».

[14] A. Santosuosso, C. Boscarato, F. Caroleo propongono un'applicazione analogica dell'art. 2048 c.c. al caso in cui un robot apprenda direttamente da un soggetto umano, considerato "insegnante" ai fini della responsabilità civile (A. Santosuosso, C. Boscarato, F. Caroleo, *Robot e diritto: una prima ricognizione*, in *Nuova giur. civ. comm.* 7-8 (2012) 513ss.). In tale prospettiva, qualora il danno fosse riconducibile a un comportamento appreso dal robot, la responsabilità ricadrebbe sul soggetto umano che ne ha curato l'addestramento. Ragionando in termini meramente civilistici, tale estensione solleva però numerosi dubbi. Da un lato, la giurisprudenza richiede, ai fini dell'esonero da responsabilità, una prova liberatoria particolarmente rigorosa, fondata sull'assoluta imprevedibilità del comportamento dell'allievo, finendo così per configurare un regime di responsabilità sostanzialmente oggettiva (cfr. E. Quarta, *Soggettività dei robots e responsibility gap*, in *La nuova procedura civile* 5 (2018) 1-21). Dall'altro, è stato osservato come tanto l'art. 2048 quanto l'art. 2047 c.c. siano stati pensati per particolari categorie di soggetti umani, disciplinando fattispecie settoriali difficilmente estendibili ad entità artificiali (D'Alfonso, *Intelligenza* cit. 171).

[15] In Crudeli, *Sistemi* cit. 424, si evidenzia come l'applicazione dell'art. 2049 c.c. al caso dell'impiego di sistemi di intelligenza artificiale nei contesti lavorativi implichi, da un lato, l'assunzione del rischio d'impresa da parte del datore di lavoro, che, decidendo di delegare determinate funzioni a un sistema autonomo, accetta consapevolmente i rischi connessi al suo utilizzo. Dall'altro lato, essa si giustifica sul piano della solvibilità, in quanto il datore rappresenta il soggetto economicamente più solido tra quelli coinvolti. In tale ottica, la norma contribuisce a superare una concezione puramente individualistica della responsabilità civile, configurandosi come espressione del principio di solidarietà sancito dall'art. 2 Cost. Infatti, come osserva E. Guardigli, tale principio assume una funzione sistemica nella società digitale, in cui la responsabilità del datore di lavoro tende ad ampliare il proprio raggio d'azione per assorbire i rischi connessi alla disintermediazione tecnologica e alla perdita di riferimenti personali nei rapporti di lavoro. In questa visione, quello che un tempo era un mero meccanismo di imputazione oggettiva si evolve ora in una responsabilità surrogatoria organizzativa, trasformandosi in uno strumento di tutela collettiva, idoneo a garantire protezione in contesti dove l'interazione tra uomo e macchina rende incerta l'individuazione del soggetto effettivamente responsabile (E. Guardigli, *La responsabilità vicaria: una rilettura alla luce dei modelli di lavoro della rivoluzione digitale*, in *Lavoro Diritti Europa* 1 (2022) 11).

[16] Ciucciovino, *La disciplina* cit. 6.

Seguendo questo approccio si potrebbe ragionevolmente ritenere che il datore abbia scientemente scelto di affidarsi ad un determinato fornitore, piuttosto che ad un altro, assumendosi quindi la responsabilità per le eventuali conseguenze derivanti dal malfunzionamento dello strumento[17]. Tale argomentazione sarebbe ulteriormente valorizzata alla luce dei principi che regolano la "law and economics", i quali tendono ad attribuire l'onere del risarcimento al soggetto economicamente più solvibile. In questo modo, la responsabilità civile non verrebbe intesa in senso puramente individualistico, quanto invece espressione del principio di solidarietà individuato dall'art. 2 Cost.[18]. Quest'ultima impostazione, pur non risolvendo i problemi legati al regime di responsabilità oggettiva, appare maggiormente coerente con l'impianto normativo che caratterizza il diritto del lavoro.

A tal fine, lo stesso Regolamento cerca di coniugare le problematiche legate al profilo di responsabilità con le esigenze di certezza del diritto, introducendo un metodo presuntivo che, sulla scia di quanto già elaborato all'interno del GDPR[19], obbliga gli utilizzatori a dotarsi di una Valutazione d'impatto sui diritti fondamentali (FRIA)[20]. Con tale documento i "deployers" sono vincolati a considerare tutte le possibili ripercussioni derivati dall'utilizzo dei sistemi di IA sotto il profilo temporale e geografico, ambientale e di governance e a formulare un piano di intervento mirato alla mitigazione dei rischi, informando se del caso i fornitori di IA e le autorità nazionali, ma anche le altre parti interessate, come le agenzie di protezione dei consumatori e le autorità di protezione dei dati[21]. Ciò apre a diverse considerazioni.

Stante le differenze sul piano applicativo con la disciplina del GDPR[22], la scelta del legislatore di affidarsi ad una valutazione preventiva appare criticabile. Dal dettato normativo non è infatti chiaro se tramite questa dichiarazione il datore possa limitare la propria responsabilità, qualora convenuto in giudizio per la violazione di diritti fondamentali. Del resto, risulta piuttosto discutibile la possibilità

[17] Ciò sarebbe peraltro in linea con l'impostazione della Cassazione per cui «in tema di responsabilità dei padroni e dei committenti ai sensi dell'art. 2049 c.c., il soggetto che, nell'espletamento della propria attività, si avvale dell'opera di terzi assume il rischio connaturato alla loro utilizzazione e, pertanto, risponde anche dei fatti dolosi o colposi di costoro, ancorché non siano alle proprie dipendenze» (Cass., Sez. III, 12/10/2018, n. 25373, Cass., Sez. III, 14/02/2019, n. 4298). Il mero rapporto di preposizione è stato inoltre esplicitato dalla Cass., Sez. III, 15/06/2016, n. 12283, secondo cui «ai fini della configurabilità della responsabilità ex art. 2049 c.c., è sufficiente che il fatto illecito sia commesso da un soggetto legato da un rapporto di preposizione con il responsabile, ipotesi che ricorre non solo in caso di lavoro subordinato ma anche quando per volontà di un soggetto (committente) un altro (commesso) esplichi un'attività per suo conto».

[18] Cfr. nota n. 15.

[19] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[20] Art. 27 del Regolamento UE 2024/1689.

[21] C. Novelli, *L'Artificial Intelligence Act Europeo: alcune questioni di implementazione*, in *federalismi.it* 2 (2024) 111-112.

[22] Per una disamina delle differenze tra la DPIA (di cui all'art. 35 del GDPR) e la FRIA vedi G. Gaudio, *Valutazioni d'impatto e management algoritmico*, in *Rivista giuridica del lavoro e della previdenza sociale* 4 (2024) 538ss. ma anche D. Fulco, *AI Act e Gdpr*, *come si rapportano: "valutazione d'impatto" e DPIA*, in *AgendaDigitale* (25/03/2024) reperibile in rete al "link" https://www.agendadigita-le.eu/cultura-digitale/ai-act-analogie-e-differenze-tra-la-valutazione-dimpatto-sui-diritti-fondamentali-fria-e-la-dpia/ e consultato il 14/03/2025. Sul punto occorre inoltre evidenziare come in ogni caso «la DPIA richieda al titolare del trattamento non solo di adottare tutte le misure appropriate necessarie per assicurare e dimostrare la conformità ai principi del GDPR, compreso il principio di trasparenza» ma anche «di valutare, mitigare e gestire i rischi per tutti i diritti e le libertà degli interessati». Così facendo «le misure da adottare devono rispondere altresì a una più ampia e ancor più pregnante esigenza di tutela, tra cui rientra quella del diritto alla dignità delle persone coinvolte» (M. Peruzzi, *Gestione algoritmica del lavoro, protezione dei dati personali e tutela collettiva*, in *Lavoro e dir.* 2 (2024) 290). Pertanto, è chiaro come la DPIA pur essendo istituita nell'ambito della disciplina per il trattamento dei dati personali, operi anche in riferimento ai diritti fondamentali.

che interessi di natura così rilevante rischino di subire una così grave limitazione da parte di una fonte di "soft law" di provenienza unilaterale.
Inoltre, l'utilizzo di tale pratica sarebbe comunque da valutare alla luce dell'impostazione adottata dalla Corte di giustizia in tema di diritti fondamentali, la quale è chiamata a giudicare a valle e non a monte del comportamento stesso[23]. Di conseguenza, qualora un imprenditore avesse correttamente adempiuto all'obbligo di redazione della FRIA, potrebbe comunque essere ritenuto responsabile di un'eventuale violazione.
D'altro canto, l'ampia discrezionalità prevista dalla normativa in capo agli utilizzatori nella redazione della stessa lascia presupporre la possibilità che essa costituisca un mero adempimento formale, più che un obbligo di natura sostanziale[24], ponendo quindi un forte interrogativo sull'effettivo valore dello strumento[25].
Alla luce di queste considerazioni, emergono più dubbi che certezze. Sebbene il regolamento sembri ridurre le responsabilità del "deployer" rispetto a quelle del "provider", il sistema normativo nel suo complesso sembra essere orientato in un'altra direzione. In questo contesto si inseriscono i nuovi strumenti di autoregolamentazione, la cui portata e i suoi effetti restano tuttavia da definire.
È dunque necessario valutare modelli di responsabilità più bilanciati, capaci di rispondere alle peculiarità del contesto lavorativo e alle sfide poste dall'innovazione tecnologica. Il dibattito resta quindi aperto.

Abstract.- Il presente contributo analizza le responsabilità del datore di lavoro nell'impiego di strumenti di intelligenza artificiale, con particolare riferimento alle implicazioni normative introdotte dall'"AI Act" e al loro impatto sul diritto del lavoro. L'analisi evidenzia il contrasto tra il modello europeo, che assegna un ruolo centrale ai fornitori di IA, e la normativa giuslavoristica nazionale, che impone al datore di lavoro obblighi di gestione e tutela dei lavoratori. In questo contesto, la distinzione tra "provider" e "deployer" solleva interrogativi circa l'attribuzione delle responsabilità, specialmente in considerazione dell'opacità dei sistemi di IA e della difficoltà di determinare le cause di eventuali danni. L'articolo esamina le possibili soluzioni giuridiche, confrontando le prospettive del diritto civile e del diritto del lavoro, e discute l'efficacia degli strumenti di autoregolamentazione introdotti dalla normativa europea. L'obiettivo è offrire una riflessione critica sulle sfide poste dall'innovazione tecnologica e individuare modelli di responsabilità più bilanciati, capaci di garantire sia la tutela dei lavoratori sia la certezza del diritto.

[23] La Corte di Giustizia dell'Unione Europea esercita un controllo a valle sul rispetto dei diritti fondamentali, valutando la compatibilità delle norme nella fase applicativa del diritto dell'Unione da parte degli Stati membri o delle istituzioni europee (art. 51, par. 1, Carta di Nizza). Infatti, «il diritto dell'Unione esclude una prassi giudiziaria che subordini l'obbligo del giudice nazionale di disapplicare una disposizione in contrasto con la Carta dei diritti fondamentali alla condizione che tale contrasto sia evidente dal suo tenore letterale o dalla giurisprudenza consolidata. Una simile limitazione priverebbe il giudice nazionale del potere di valutare pienamente la compatibilità della norma con la Carta, eventualmente con il supporto della Corte di Giustizia» (Corte UE, 26/02/2013, Åkerberg Fransson, C-617/10). Questo principio si applica anche nei rapporti tra privati in quanto i diritti fondamentali dell'UE godono di efficacia diretta orizzontale (Corte UE, 19/04/2016, Dansk Industri, C-441/14).
[24] Novelli, *L'Artificial intelligence* cit. 111-112.
[25] Anche alla luce del fatto che la valutazione deve essere sempre consegnata all'autorità di vigilanza (art. 27, par. 3, del Regolamento), ovvero ipotizzando una valenza non solo interna dello strumento.

This paper examines employer liability in the use of artificial intelligence (AI) tools, with a particular focus on the regulatory implications introduced by the AI Act and its impact on labor law. The analysis highlights the contrast between the European model, which assigns a central role to AI providers, and national labor regulations, which place managerial and protective duties on employers. In this context, the distinction between “providers” and “deployers” raises questions about liability attribution, especially considering the opacity of AI systems and the difficulty in determining the causes of potential harm. The paper explores possible legal solutions by comparing civil and labor law perspectives and discusses the effectiveness of self-regulatory mechanisms introduced by European regulations. The goal is to provide a critical reflection on the challenges posed by technological innovation and to identify more balanced liability models that ensure both worker protection and legal certainty.