

■ **MARZIA BARBERA ANALIZZA L'IMPATTO DELLE INNOVAZIONI DIGITALI SUL RISCHIO E SULLA RESPONSABILITÀ NELL'IMPRESA (ANCHE ALLA LUCE DELLE POSIZIONI UE)**

# RISCHIO E RESPONSABILITÀ al tempo dell'impresa digitale\*

• A CURA DI LUCA DI SEVO *Consulente del Lavoro in Bollate (Mi)* •

“L’innovazione digitale ha rimesso al centro del diritto del lavoro la questione del rischio e della responsabilità e di come il diritto possa governare i possibili vantaggi e i potenziali rischi connessi alla tecnologia digitale applicata al lavoro umano e a chi assegnare la responsabilità del verificarsi di un danno”. Il diritto del lavoro digitale si presenta particolarmente complesso ed in costante evoluzione; inoltre, costringe a combinare principi normativi non lavoristici, con garanzie tipiche del diritto del lavoro (ad esempio sicurezza sul lavoro o *privacy*) e ad utilizzare pratiche *risk-management* per la gestione del rischio tecnologico. Infine, molte aziende adottano spontaneamente codici di condotta su base volontaria.

Il diritto del lavoro digitale si presenta prevalentemente “*risk-based*” e può essere visto come un meccanismo di redistribuzione dei rischi di mercato e dei rischi sociali.

Alcuni elementi caratteristici possono essere individuati come segue: “l’adozione di una concezione graduata di rischio; la distribuzione del rischio fra le due parti del rapporto piuttosto che l’attribuzione a quella economicamente più forte; l’affidamento della gestione del rischio a un’auto-regolazione di natura privata, di carattere prevalentemente procedurale, di natura flessibile e dagli esiti aperti”.

“La *“pyramid of criticality”* adottata dalla Proposta di regolamento sull’IA (da ora, il Rego-

lamento), propone un livello di “basso rischio”, in cui non si applica nessuna limitazione all’uso degli strumenti tecnologici; un livello di “rischio limitato”, in cui vigono soltanto obblighi di trasparenza; un livello di “alto rischio” a cui corrisponde una serie di restrizioni più o meno rigorose; infine, in cima alla piramide, un livello di “rischi inaccettabili” che il sistema vieta tassativamente di assumere (es. la messa in servizio o l’uso di un sistema di IA che sfrutta le vulnerabilità di uno specifico gruppo di persone, dovute all’età o alla disabilità fisica o mentale)”.

Secondo il Regolamento si classificano come “sistemi ad alto rischio” quelli utilizzati per l’assunzione e la selezione delle persone, per l’adozione di decisioni in materia di promozione e cessazione del rapporto di lavoro, per l’assegnazione dei compiti, per il monitoraggio o la valutazione delle persone nei rapporti contrattuali legati al lavoro. La motivazione è data dal fatto che questi strumenti possono essere determinanti per le future prospettive di carriera, per generare situazioni di discriminazione. I sistemi per monitorare le prestazioni e il comportamento di tali persone possono incidere sui loro diritti in materia di protezione dei dati e vita privata.

In ogni caso, l’impresa deve garantire grazie all’apporto umano, di sviscerare ogni situazione e decidere, se e quando non utilizzare un sistema di IA ad alto rischio oppure se e quan- ➤

\* Sintesi dell’articolo pubblicato in *Labour&LawIssues*, vol. 9, no. 2, 2023 dal titolo “*La nave deve navigare*”. *Rischio e responsabilità al tempo dell’impresa digitale*.

## RISCHIO E RESPONSABILITÀ AL TEMPO DELL'IMPRESA DIGITALE

do ignorare, annullare o ribaltare l'*output* del sistema stesso: si può definire questo approccio come principio di umanizzazione.

Le tecniche moderne di valutazione attribuiscono il rischio alle due parti, sulla base di valutazioni di tipo procedurale (*risk assesment e planning*) e rendicontazioni concrete.

Nel Regolamento viene suggerito il bilanciamento fra interesse dell'impresa e interesse della persona utilizzando il criterio della riduzione al minimo dei costi per la protezione della persona: si applica un "approccio normativo orizzontale all'IA equilibrato e proporzionato, che si limita ai requisiti minimi necessari per affrontare i rischi e i problemi ad essa collegati, senza limitare od ostacolare indebitamente lo sviluppo tecnologico o altrimenti aumentare in modo sproporzionato il costo dell'immissione sul mercato di soluzioni di IA".

Nell'approccio del *risk management* l'evento da evitare è la mancata (o scarsa) capacità di anticipare e prevenire (o attenuare) un evento prevedibile e, in assenza di danni e in caso di controlli dell'autorità, quello dell'aver applicato misure di sicurezza non adeguate al rischio calcolato o del non aver saputo rendicontare la propria attività e, di conseguenza, del non essere in grado di dimostrare di aver fatto tutto il possibile per (provare a) evitare il danno. L'imprenditore, in sostanza, non è responsabile per l'effettivo verificarsi del danno, ma è responsabile per non averlo previsto e prevenuto. Secondo il Regolamento, in sintesi, l'evento deve essere prevedibile e noto (tipici principi della responsabilità) e il controllo deve essere possibile e non eccessivamente oneroso.

Il Regolamento propone un "approccio proporzionato basato sul rischio prevedibile".

Si stabilisce così una gradazione dei rischi e dei costi che implica la loro eliminazione o riduzione sulla base di una serie di considerazioni che devono essere oggetto di discernimento in termini utilitaristici ma anche valoriali.

Al centro, viene messa la dignità della persona. Ad esempio, in biotecnologia (Direttiva europea 98/94 CE) la protezione giuridica delle invenzioni biotecnologiche esclude la brevettabilità di invenzioni contrarie all'ordine pubblico e al buon costume (come i procedimenti di clonazione di esseri umani). Nelle tecnologie digitali, il Regolamento vieta (salvo specifiche eccezioni) il ricorso al riconoscimento biometrico in tempo reale. In altri casi, si opta per il bilanciamento.

La fiducia è un secondo aspetto. Il Regolamento segnala, fra le sue priorità quella di «favorire lo sviluppo di un ecosistema di fiducia nei confronti dell'IA in Europa», di garantire che i sistemi di IA siano «sicuri e affidabili».

Queste nuove concezioni del rischio e della responsabilità lasciano intravedere un'idea di impresa sensibile sia ad aspetti sociali che politici. Sotto il profilo sociale, l'impresa deve risultare affidabile, deve assicurare "trasparenza" (intesa come garanzia della completa accessibilità alle informazioni e come capacità di rendere conto a *stakeholders* e *shareholders* di scelte, comportamenti e azioni). Tale dimensione organizzativa e sociale richiede che si prenda in considerazione il funzionamento responsabile dell'organizzazione, la creazione di fiducia e la presa in carico di interessi e scopi diversi da interessi prettamente economici.

In chiave politica, l'impresa è un soggetto dotato di poteri di regolazione e controllo, e deve essere anche il tramite dell'esercizio e della tutela di diritti della persona.

A parere di chi si è occupato della sintesi di questo lavoro, il tema è molto delicato e necessita molta attenzione da parte di tutti gli attori coinvolti. Si parla sempre più insistentemente di Intelligenza Artificiale e dei suoi possibili sviluppi. È necessario, tuttavia, concentrarsi non solo sugli aspetti utilitaristici di questa evoluzione informatica, ma anche su tanti altri temi di natura etica e sociale.