

segue da pag. 1 →

AI in azienda: il quadro normativo e la proprietà intellettuale

sia a livello corporate che personale?

I rischi sono concreti e operano su più livelli. Sul piano civile, l'impresa risponde per i danni causati dai propri ausiliari, inclusi quelli tecnologici, ai sensi dell'art. 55 CO. Se un sistema di IA genera un output errato - ad esempio una consulenza fiscale basata su una norma abrogata, o un report con dati inventati (le cosiddette "allucinazioni") - il danno ricade sull'azienda che ha utilizzato quello strumento e ha fornito l'output al cliente. L'IA non è un soggetto giuridico: non può essere citata in giudizio, non ha patrimonio, non ha responsabilità. La responsabilità è sempre dell'impresa e delle persone fisiche che la dirigono. Sul piano civilistico, l'impresa può anche rispondere per *culpa in eligendo* (cattiva scelta del fornitore o dello strumento) e *in vigilando* (insufficiente controllo sull'output), ai sensi degli artt. 41 ss. CO.

Sul piano personale, il Consiglio di Amministrazione ha responsabilità intrasmissibili di alta direzione e vigilanza (art. 716a CO). Ignorare che i dipendenti utilizzano strumenti di IA - fenomeno noto come "shadow AI" - può configurare una *culpa in vigilando*. Se un collaboratore carica dati sensibili su una piattaforma IA non autorizzata e questi vengono compromessi, il CdA potrebbe dover rispondere per negligenza organizzativa. Il principio è chiaro: l'IA può supportare, ma mai sostituire, la responsabilità decisionale dei dirigenti.

Sul versante penale, i rischi emergono principalmente nel trattamento dei dati personali. La nLPD prevede sanzioni penali (fino a CHF 250'000 per le persone fisiche responsabili) in caso di violazione intenzionale degli obblighi di informazione, dei doveri di diligenza o del segreto professionale. L'IA può anche generare contenuti che riproducono opere protette, codici proprietari o informazioni riservate, esponendo l'azienda a violazioni della proprietà intellettuale e della Legge contro la concorrenza sleale (LCSI, artt. 4 e 6). Un utilizzo non governato può inoltre esporre documenti aziendali a vulnerabilità e rischi di cybersecurity, anche dovuti a semplice errore umano.

Un ulteriore rischio specifico per chi opera nell'ambito HR riguarda i risultati discriminatori: se un sistema IA utilizzato per lo screening dei CV o la valutazione del merito creditizio produce output distorti - ad esempio penalizzando candidati per genere, età o provenienza - le conseguenze possono essere rilevanti sul piano giuslavoristico, con decisioni distorte che violano il principio di buona fede (art. 328 CO), e possono dar luogo a pretese risarcitorie o indennità in fase di assunzione o gestione del rapporto. A ciò si aggiunge un significativo rischio reputazionale. Occorre inoltre considerare che le decisio-

ni che incidono su aspetti essenziali del rapporto di lavoro - dalla selezione del personale all'avanzamento di carriera, sino al termine del rapporto - non possono essere completamente automatizzate: occorre garantire la revisione umana e la possibilità di contestazione degli output.

Quali sono i riflessi dell'IA sulla proprietà intellettuale, i segreti industriali e commerciali, e i dati personali?

Sono tre ambiti distinti che l'IA impatta simultaneamente, e che richiedono una strategia integrata.

Proprietà intellettuale. La LDA svizzera, così come la normativa UE, richiede che l'opera sia il frutto di una "creazione intellettuale con carattere individuale" di un autore umano. L'output generato esclusivamente da un algoritmo - senza un intervento creativo umano significativo - non è protetto dal diritto d'autore e ricade nel pubblico dominio. Un concorrente potrebbe copiarlo liberamente. Il punto critico è la documentazione: per rivendicare la protezione, l'azienda deve poter dimostrare che l'intervento umano è stato sostanziale - selezione, editing, composizione, post-produzione - e non limitato alla semplice digitazione di un prompt generico. In ambito UE, la Direttiva 2019/790 sul Copyright Digitale regola l'uso di opere protette per l'addestramento dei modelli IA attraverso il Text and Data Mining (TDM), garantendo ai titolari dei diritti il cruciale diritto di opt-out.

Segreti industriali e commerciali. Questo è forse il rischio meno percepito e più insidioso. Ogni volta che un dipendente inserisce in un modello IA dati strategici - listini prezzi, formule, codici sorgente, piani commerciali - esiste il rischio concreto che queste informazioni vengano utilizzate per l'addestramento del modello o siano accessibili a terzi. Il segreto commerciale, tutelato dalla LCSI, perde la sua protezione nel momento in cui non è più "segreto". L'utilizzo di versioni enterprise con clausole di non-addestramento (opt-out) e zero data retention (ZDR) è un requisito minimo di diligenza. Al contempo, i prompt complessi sviluppati internamente - contenenti istruzioni stratificate, logiche proprietarie e dati storici - possono e devono essere trattati come segreti commerciali, con accesso ristretto e clausole di riservatezza nei contratti con dipendenti e consulenti.

Dati personali. La nLPD impone che l'uso dell'IA per trattare dati personali rispetti i principi di minimizzazione, trasparenza e finalità. Prima di implementare uno strumento IA che tratta dati personali, è obbligatorio redigere una valutazione d'impatto sulla protezione dei dati (DPIA), trattandosi di un trattamento ad "alto rischio". Occorre verificare dove risiedono fisicamente i server del fornitore - preferibilmente in Svizzera o nell'UE - e assicurarsi che i dati non vengano utilizzati per scopi diversi da quelli dichiarati. Nel contesto HR, in particolare, ogni forma di sorveglianza deve rispettare l'art. 26 OLL 3: nessun controllo occulto è ammesso, salvo che sia proporzionato e dichiarato anticipatamente ai lavoratori.

Come vanno considerati i contenuti genera-

ti dall'IA stessa?

Questo è il nodo giuridico centrale del momento. La risposta varia a seconda della giurisdizione, e il quadro internazionale è tutt'altro che uniforme. Il principio generale, valido in Svizzera e nell'UE, è che il diritto d'autore tutela esclusivamente le creazioni umane. Un contenuto generato interamente dall'IA, senza apporto creativo umano significativo, non è proteggibile e ricade nel pubblico dominio. L'IA non è un soggetto giuridico e non può essere titolare di diritti. A livello internazionale, emergono due approcci contrapposti. Gli Stati Uniti adottano una posizione rigida: lo U.S. Copyright Office ha stabilito che solo gli esseri umani possono essere autori e che la mera fornitura di un prompt non costituisce un atto creativo sufficiente. Questa posizione è stata confermata nel caso *Thaler v. Perlmutter* (2023) e nel caso *Zarya of the Dawn*, dove la protezione è stata negata alle illustrazioni generate dall'IA, sebbene il testo umano e l'organizzazione complessiva dell'opera fossero proteggibili. La Cina, invece, ha adottato un approccio più aperto. Nel caso *Li Yunkai* (Tribunale di Pechino, 2023), il giudice ha riconosciuto la protezione del copyright a un'immagine generata con *Stable Diffusion*, sulla base del fatto che l'utente aveva elaborato oltre 150 prompt, organizzandoli in un ordine specifico e intervenendo ripetutamente fino a ottenere il risultato desiderato. Il tribunale ha qualificato questa attività come "investimento intellettuale significativo", paragonandola al lavoro di un fotografo che regola manualmente l'apparato. Ha anche compiuto un paragone illuminante: mentre un pittore incaricato mantiene una propria volontà e uno stile personale, il software IA non possiede né volontà soggettiva né gusto personale. Per l'impresa, la lezione operativa è triplice. Primo: l'output grezzo dell'IA non va considerato un asset protetto. Secondo: per ottenere protezione, è necessario documentare analiticamente l'apporto umano - dal prompting avanzato alla selezione, fino all'editing sostanziale. Terzo: in ambito UE, l'AI Act impone la marcatura dei contenuti generati dall'IA, creando un obbligo di trasparenza che si applica indipendentemente dalla questione della paternità. Un'azienda che pubblica contenuti IA senza etichettarli rischia una doppia esposizione: assenza di protezione IP e sanzioni per mancata trasparenza. Anche le grandi piattaforme si stanno adeguando: Meta, ad esempio, richiede già l'etichettatura per video e audio realistici generati dall'IA su Instagram.

IMPRESSUM

Newsletter **Lavoro** è la pubblicazione mensile del sistema d'informazione **Il diritto del lavoro applicato**.
Editore: Boss Editore SA
Resp. Newsletter: Gian Luigi Trucco
Hanno collaborato: Gianvirgilio Cugini, Giorgia Collina, Christopher Jackson e Luca Orsatti
Boss Editore SA - CH 6900 Lugano
tel. +41(0)91 600 93 03
Amministrazione: info@boss-editore.ch
© www.boss-editore.ch

AI in azienda: aspetti operativi

Intervista all'Avv. Giorgia Collina, dello Studio Legale Cugini di Lugano



dipendenti (la cosiddetta "shadow AI"). È frequente che collaboratori utilizzino versioni gratuite di chatbot per attività lavorative, caricando inconsapevolmente dati sensibili su piattaforme esterne senza alcun controllo aziendale. Il secondo passo è la redazione di una AI Policy aziendale chiara e accessibile a tutti i collaboratori. Questo documento deve definire con chiarezza quali strumenti sono autorizzati, quali dati possono essere inseriti e quali no, e quali processi richiedono la validazione umana prima della diffusione dell'output. Le categorie di informazioni che nei regolamenti devono chiaramente essere indicate come escluse categoricamente dai sistemi AI includono: dati personali sensibili di clienti o dipendenti, password e credenziali, segreti industriali o formule proprietarie, codici sorgente e documentazione tecnica riservata. Anche in questo caso è importante per l'azienda poter comprovare la sua politica proattiva adottando un framework completo per tracciare decisioni, dati e test. Il terzo passo riguarda i contratti. I contratti di lavoro e di collaborazione vanno integrati con appendici specifiche sull'uso delle tecnologie emergenti, richiamando il dovere di fedeltà e diligenza previsto dall'art. 321a CO. I contratti con i fornitori di software IA devono prevedere clausole sulla proprietà dei dati e degli output, sulla residenza dei server, sulla zero data retention e sulla conformità all'AI Act per le attività destinate al mercato UE. Il quarto passo è la formazione. Non si tratta di insegnare la tecnica, ma di sensibilizzare i manager e i collaboratori sulla responsabilità legale connessa all'uso dell'AI e sulla capacità critica di valutare l'output. Il principio fondamentale è il "human-in-the-loop": l'AI suggerisce, l'umano decide e si assume la responsabilità. Ogni report generato con supporto AI dovrebbe recare la dicitura "analizzato con supporto tecnologico, validato da [Nome Professionista]".

In un contesto in cui molte PMI si sentono sopraffatte dalla complessità normativa, qual è il valore concreto di dotarsi oggi di una governance AI strutturata e quale ruolo può svolgere uno studio legale specializzato?

Questa è la domanda che dovrebbe porsi ogni imprenditore e la risposta va contro un pregiudizio diffuso: la governance dell'AI non è un costo, è un investimento che produce valore misurabile. Siamo consapevoli che questo tipo di

attività si traduce in un costo per le aziende ma la conformità alle norme e alle best practice diventano vantaggio competitivo in un mondo in cui il progresso tecnologico non può essere ignorato. Il primo valore è la protezione del patrimonio aziendale. Senza una policy interna, l'azienda rischia ogni giorno la dispersione dei propri segreti commerciali attraverso l'uso incontrollato di strumenti AI da parte dei dipendenti. Senza protocolli di documentazione dell'apporto umano, gli output creativi generati con l'AI rimangono nel pubblico dominio, vulnerabili alla copia. Senza clausole contrattuali adeguate con i fornitori, l'azienda non ha strumenti di rivalsa in caso di problemi. Ognuna di queste lacune rappresenta una perdita patrimoniale potenziale. Colmarie ha un costo contenuto rispetto al danno che previene. Vi è poi un valore competitivo. Le PMI ticinesi che operano con l'UE si troveranno presto a dover dimostrare la conformità all'AI Act nei rapporti commerciali con partner e clienti europei. Chi si struttura per primo acquisisce un vantaggio: la compliance diventa un argomento di vendita, non un ostacolo. Allo stesso modo, un'azienda che può certificare ai propri clienti un processo di utilizzo responsabile dell'AI si differenzia sul mercato in termini di affidabilità e reputazione. Infine, si crea un valore di tipo organizzativo. L'AI può diventare un acceleratore del passaggio generazionale, un tema cruciale per molte PMI familiari del Ticino. Utilizzare l'AI per mappare e digitalizzare il know-how tacito del fondatore (processi, relazioni, logiche decisionali) attraverso una base di conoscenza interna interrogabile, significa creare un asset aziendale che sopravvive alla singola persona. Ma questo processo deve avvenire in sicurezza: la base di conoscenza deve essere crittografata, l'accesso regolato e il sistema protetto da clausole di riservatezza rigorose. Il ruolo di uno studio legale specializzato, in questo contesto, non è quello di frenare l'innovazione, ma di renderla sostenibile. Il nostro approccio è quello di affiancare l'imprenditore in un percorso che arrivi alla costruzione di strumenti operativi su misura. Non esistono soluzioni preconfezionate: ogni azienda ha un profilo di rischio diverso, un mercato diverso, una cultura interna diversa. La governance dell'AI deve essere sartoriale, non industriale. Il punto di partenza è sempre una conversazione strategica: capire dove l'azienda vuole andare con l'AI e costruire il percorso legale per arrivarci in sicurezza.

Si sono già verificati casi concreti di contenzioso?

Sì, e sono istruttivi proprio perché dimostrano come i rischi teorici si traducano in conseguenze pratiche. Oltre a quelli già citati dall'Avv. Cugini, in ambito europeo, il caso attualmente più rilevante è *Like Company v. Google Ireland* (C-250/25). L'editore ungherese ha convenuto in giudizio Google Ireland sostenendo che il chatbot Gemini riproducesse i suoi articoli protetti da copyright senza autorizzazione, generando riassunti dettagliati su richiesta degli utenti. La Corte di Giustizia UE si trova ora a decidere se l'addestramento di un LLM e i suoi output costituiscano "riproduzione" e "comunicazione al pubblico" ai sensi delle direttive europee sul diritto d'autore. Vi sono poi altri casi venuti alla luce di professionisti che affidandosi all'AI hanno citato sentenze e fonti inesistenti, creando danni ai propri clienti e alla propria reputazione. Il dato comune è che in nessuno di questi casi il problema è la tecnologia in sé, ma l'assenza di governance, di supervisione umana e di documentazione.