Dal DVR all'AI Literacy: intersezioni normative tra Regolamento (UE) 2024/1689, Digital Omnibus, Legge n. 132/2025 e D.Lgs. n. 81/2008 nella tutela dei lavoratori.

L'INTEGRAZIONE DEI SISTEMI DI INTELLIGENZA ARTIFICIALE AD ALTO RISCHIO NELLE PROCEDURE AZIENDALI DI TUTELA DELLA SALUTE E SICUREZZA SUL LAVORO

*di Francesco Di Bono**

Il presente contributo analizza e approfondisce le articolate implicazioni dogmatiche ed operative derivanti dall'introduzione nei contesti organizzativo-aziendali dei sistemi di Intelligenza Artificiale ad alto rischio. Il saggio esamina in chiave coordinata l'intersezione eurounitaria e nazionale tra la regolamentazione dell'*AI Act* (Regolamento UE 2024/1689), le più recenti riforme introdotte dal *Digital Omnibus* (Regolamento UE 2026/1744), il quadro normativo di sistema della Legge 23 settembre 2025, n. 132 e i relativi decreti attuativi, unitamente al sistema generale di prevenzione e protezione di cui al D.Lgs. 9 aprile 2008, n. 81. Attraverso una disamina sistematica, il lavoro mappa l'obbligo datoriale di aggiornamento del Documento di Valutazione dei Rischi (DVR), le dinamiche procedimentali legate al coinvolgimento partecipativo del Rappresentante dei Lavoratori per la Sicurezza (RLS), la riserva assoluta di funzione riservata all'atto medico-legale del Medico Competente e le declinazioni operative in tema di sorveglianza funzionale e alfabetizzazione algoritmica dei lavoratori (*AI Literacy*).

Sommario

1. La convergenza sistematica tra il diritto dell'Unione e il T.U. Sicurezza sul Lavoro.
2. Il Documento di Valutazione dei Rischi: analisi dei tre profili di rischio emergente.
3. La consultazione dell'RLS: procedimento, tempistiche e poteri partecipativi.
4. Il raccordo con il medico competente: la riserva di funzione e il confine dell'art. 41 D.Lgs. n. 81/2008.
5. La sorveglianza funzionale e la nuova disciplina dell'AI Literacy dopo il Digital Omnibus.
6. Profili sanzionatori, responsabilità 231 e quadro della compliance integrata.
7. Conclusioni.

The paper examines in depth the operational implications stemming from the deployment of high-risk Artificial Intelligence systems within corporate-organizational contexts. The study examines, in an integrated framework, the EU and national intersection between the AI Act regulation (Regulation EU 2024/1689), the most recent reforms introduced by the Digital Omnibus (Regulation EU 2026/1744), the systemic regulatory framework of Law no. 132 of September 23, 2025, and its implementing decrees, alongside the general prevention and protection system set forth in Legislative Decree no. 81 of April 9, 2008. Through a systematic analysis, the work maps the employer's obligation to update the Risk Assessment Document (DVR), the procedural dynamics related to the participatory involvement of the Workers' Health and Safety Representative (RLS), the absolute functional reservation assigned to the medico-legal act of the competent physician and the operational applications concerning functional surveillance and workers' algorithmic literacy (AI Literacy).

*Funzionario ITL Bari - Le considerazioni contenute nel presente contributo sono frutto esclusivo del pensiero dell'Autore e non hanno carattere impegnativo per l'Amministrazione di appartenenza.

ISSN 3035-4846

L'introduzione di un sistema di Intelligenza Artificiale (IA) ad alto rischio nei luoghi di lavoro — con particolare riguardo alle tipologie mappate all'Allegato III, punti 3 e 4, del Regolamento (UE) 2024/1689 (*AI Act*)[1], inerenti all'istruzione, alla formazione professionale, alla gestione dei lavoratori e all'accesso al lavoro autonomo — travalica ampiamente i confini del mero acquisto o ammodernamento tecnologico. Essa costituisce un vero e proprio "evento organizzativo complesso" idoneo a riconfigurare la mappa dei rischi aziendali e la catena di responsabilità di cui al D.Lgs. 9 aprile 2008, n. 81[2]. Sul piano dell'inquadramento dogmatico, la disciplina sovranazionale dell'*AI Act* e quella di fonte interna (D.Lgs. n. 81/2008) operano secondo una logica di integrazione multilivello e di cumulabilità degli adempimenti.

Se il regolamento europeo presidia primariamente la conformità di prodotto, la trasparenza degli algoritmi e la tutela dei diritti fondamentali contro le derive della sorveglianza di massa o del pregiudizio discriminatorio, la normativa nazionale recepisce l'innovazione tecnologica all'interno del perimetro dell'art. 2087 c.c. e dell'art. 15 D.Lgs. n. 81/2008, imponendo la valutazione globale e prospettica di tutti i fattori di rischio derivanti dalle scelte organizzative e produttive del datore di lavoro.

Un elemento di precipua rilevanza teorica e applicativa risiede nella gestione delle sfalsate tempistiche di efficacia normativa: da un lato, le prescrizioni del D.Lgs. n. 81/2008 in materia di valutazione dei rischi, informativa ai lavoratori, consultazione delle rappresentanze e sorveglianza sanitaria sono immediatamente esigibili dal momento preciso in cui la nuova tecnologia fa il suo ingresso nel ciclo aziendale; dall'altro lato, gli obblighi specifici posti dall'art. 26 dell'*AI Act* in capo al *deployer* (ovvero all'utilizzatore professionale del sistema ad alto rischio) divengono pienamente cogenti a far data dal 2 dicembre 2027 per i sistemi dell'Allegato III, a seguito del differimento delle decorrenze del Capo III operato dall'art. 113 del Regolamento (UE) 2026/1744 (*Digital Omnibus*).

Cionondimeno, l'impostazione aziendale non può cedere a una fuorviante scissione procedurale: l'adozione di un approccio di *AI Governance* integrata e di tutela preventiva richiede che il datore di lavoro conformi la propria documentazione e i propri flussi di sicurezza ai requisiti europei fin dal momento del primo impianto.

1. La convergenza sistematica tra il diritto dell'Unione e il T.U. Sicurezza sul Lavoro

[1] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828, in GUUE L, 2024/1689, 12 luglio 2024.

[2] D.Lgs. 9 aprile 2008, n. 81 e s.m.i., Attuazione dell'articolo 1 della legge 3 agosto 2007, n. 123, in materia di tutela della salute e della sicurezza nei luoghi di lavoro, in G.U. n. 101 del 30 aprile 2008 - Suppl. Ordinario n. 108.

2. Il Documento di Valutazione dei Rischi: analisi dei tre profili di rischio emergente

Ai sensi dell'art. 28 del D.Lgs. n. 81/2008, la valutazione dei rischi deve riguardare «tutti i rischi per la sicurezza e la salute dei lavoratori», ivi compresi quelli collegati allo stress lavoro-correlato, alle differenze di genere, all'età e alla provenienza da altri Paesi. L'art. 17, comma 1, lett. a), qualifica la valutazione dei rischi e l'elaborazione del relativo documento (DVR) come un obbligo personale e non delegabile del datore di lavoro.

Ne consegue che la predisposizione di una Sezione Speciale del DVR dedicata all'Intelligenza Artificiale non può essere trasferita integralmente a consulenti esterni o al fornitore del software, rimanendo la titolarità della decisione organizzativa in capo al vertice aziendale. L'introduzione di un sistema di IA ad alto rischio impone l'identificazione, l'analisi e la misurazione di tre specifici profili di rischio emergenti:

A) Profilo 1 — Rischio da output non supervisionato (o da erogazione di decisioni automatizzate). Qualora il sistema algoritmico rilasci indicazioni od output (es. punteggi di rendimento, pianificazione dei turni, valutazione dell'idoneità tecnica o raccomandazioni formative) e tali dati vengano recepiti in modo acritico o automatizzato dalla linea gerarchica, si genera un grave rischio per la salute e la sicurezza. Un errore di profilazione algoritmica può condurre all'assegnazione di mansioni gravose o pericolose a soggetti non idonei, ovvero all'ingiustificata estromissione di lavoratori esperti con conseguente decadimento dello stato psicofisico e professionale. Il DVR deve pertanto descrivere la metodologia adottata per misurare la probabilità dell'errore algoritmico e le barriere organizzative frapposte a presidio della decisione finale.

B) Profilo 2 — Rischio da *bias* algoritmico e discriminazione sistemica. I modelli statistico-predittivi vengono addestrati su dataset che storicamente possono incorporare o riprodurre pregiudizi impliciti. Se il dataset d'addestramento non rispecchia la composizione reale della forza lavoro (es. sottorappresentazione di lavoratrici donne, lavoratori anziani o lavoratori stranieri), il sistema produrrà valutazioni sistematicamente penalizzanti per tali categorie. Poiché l'art. 28 D.Lgs. n. 81/2008 richiede espressamente di valutare i rischi in funzione del genere, dell'età e della provenienza, la gestione del *bias* rientra pienamente nella prevenzione antinfortunistica e di tutela della salute. In questo contesto si inserisce la norma d'eccezione recata dall'art. 4-bis del Regolamento (UE) 2024/1689[3] (introdotta e consolidata a livello eurounitario), la quale riconosce al *deployer* la base giuridica per trattare, in via straordinaria e sotto strette garanzie di riservatezza, categorie particolari di

[3] L'Articolo 4-bis è stato introdotto all'interno del Regolamento (UE) 2024/1689 (AI Act) dal recente Regolamento (UE) 2026/1744 (Digital Omnibus sull'IA), in GUUE L, 2026/1744, 24 luglio 2026. Si colloca nel Capo I (Disposizioni Generali) subito dopo l'art. 4 (Alfabetizzazione in materia di IA) ed è intitolato «Trattamento di categorie particolari di dati personali per il rilevamento e la correzione delle distorsioni». Introduce la disciplina per la gestione e la mitigazione del bias algoritmico mediante l'uso controllato di dati particolari/sensibili, raccordando la compliance AI Act con i requisiti del Regolamento (UE) 2016/679 (GDPR).

ISSN 3035-4846

dati personali al solo ed esclusivo fine di rilevare e correggere distorsioni (*bias*) nei sistemi ad alto rischio. Si tratta di una facoltà d'indagine tecnica a disposizione dell'organizzazione per garantire la trasparenza e l'equità dei processi di valutazione.

C) Profilo 3 — Rischio da tracciamento fisiologico, comportamentale e stress lavoro-correlato. L'impiego di sensori indossabili (*wearables*), telecamere con analisi della postura o sistemi di monitoraggio continuo del flusso di lavoro determina una pervasiva ingerenza nella sfera personale dell'operatore. La percezione di essere costantemente sottoposti al giudizio dell'algoritmo attiva forme latenti o acute di stress lavoro-correlato, sindromi da *burnout* e deterioramento del clima relazionale. Il datore di lavoro ha l'obbligo di valutare la portata psicosociale di tale monitoraggio, predisponendo pause programmate, schermature dei dati e garanzie circa il divieto assoluto di utilizzare dati di monitoraggio comportamentale per finalità disciplinari o per inferenze emotive vietate dall'art. 5 dell'AI Act.

La strutturazione della specifica Sezione del Documento di Valutazione dei Rischi (DVR) dedicata ai sistemi di Intelligenza Artificiale presuppone un'articolazione metodologica e contenutistica rigorosa, volta a coniugare le prescrizioni della disciplina prevenzionistica di cui al D.Lgs. 81/2008 con le istanze regolatorie introdotte dal Regolamento (UE) 2024/1689 (AI Act). Per garantire l'esaustività formale e la tenuta dogmatica del documento, la mappatura dei contenuti minimi della Sezione IA deve svilupparsi attraverso dieci direttrici costitutive ed essenziali.

In primo luogo, il documento deve muovere dall'identificazione puntuale del sistema di IA, specificandone la denominazione, la versione software, l'entità fornitrice e lo specifico ambito operativo di inserimento; in tale sede si rende altresì necessaria la perimetrazione delle tipologie di dati trattati e la precisa individuazione delle categorie di lavoratori interessate dal funzionamento dell'algoritmo.

A tale inquadramento descrittivo segue la classificazione del sistema alla luce della normativa eurounitaria (AI Act), che richiede l'esplicita sussunzione della fattispecie in una delle ipotesi previste dall'Allegato III del Regolamento, previa rigorosa verifica circa l'assenza di pratiche vietate ai sensi dell'art. 5, unitamente al quadro temporale di decorrenza dei relativi obblighi. Il cuore valutativo della Sezione si sostanzia nella triplice stima dei rischi emergenti, in cui il datore di lavoro è chiamato a ponderare probabilità e gravità del danno con riguardo a tre fenomeni critici: le deviazioni derivanti da output privi di adeguata supervisione, l'insorgenza di *bias* ed errori algoritmici, e le implicazioni legate al tracciamento comportamentale dei lavoratori. Per fronteggiare tali elementi di rischio, il DVR deve codificare idonee misure di prevenzione e protezione, declinando procedure operative volte a contenere le criticità rilevate, nel rispetto dei vincoli d'uso indicati dal fabbricante e mediante la predisposizione di adeguate garanzie di cybersecurity. Sotto il profilo formale e

documentale, la validità della Sezione è subordinata alla corretta tenuta e archiviazione della documentazione tecnica, con particolare riferimento alle istruzioni d'uso fornite dal produttore ai sensi dell'Allegato IV dell'AI Act e alla presenza della dichiarazione di conformità CE. A ciò si affianca la disciplina della sorveglianza funzionale e del controllo umano (human oversight), che impone l'individuazione formale del personale preposto alla supervisione dell'IA, la definizione di un chiaro protocollo per la gestione dei malfunzionamenti o delle anomalie e la strutturazione di un sistema di tracciamento e conservazione dei log.

Il profilo procedimentale e partecipativo si articola, in primo luogo, nella fase dell'informativa ai lavoratori, della cui avvenuta somministrazione occorre dare prova tracciabile (ai sensi dell'art. 36 del D.Lgs. 81/2008 e in vista del completo dispiegarsi degli obblighi di cui all'art. 26 dell'AI Act). In secondo luogo, assume valore dirimente la consultazione preventiva del Rappresentante dei Lavoratori per la Sicurezza (RLS), le cui dinamiche devono essere debitamente formalizzate mediante apposito verbale che dia conto delle osservazioni formulate e delle correlate motivazioni datoriali. Particolare rilievo teorico e sistematico assume il raccordo con la funzione del medico competente: la Sezione IA del DVR deve infatti sancire un invalicabile protocollo organizzativo diretto a scindere nettamente le valutazioni di prestazione rese dall'IA dal giudizio medico-legale sull'idoneità alla mansione specificamente riservato allo specialista ex art. 41 del D.Lgs. 81/2008.

Infine, stante la natura intrinsecamente evolutiva delle tecnologie algoritmiche, il documento deve definire un programma di aggiornamento periodico e dinamico, stabilendo scadenze di revisione con cadenza almeno annuale, nonché l'obbligo di rielaborazione immediata al verificarsi di modifiche sostanziali nell'architettura del software o negli assetti dell'organizzazione del lavoro.

3. La consultazione dell'RLS: procedimento, tempistiche e poteri partecipativi

La partecipazione dei lavoratori al processo di gestione della sicurezza tramite il Rappresentante dei Lavoratori per la Sicurezza (RLS) rappresenta un principio cardinale del modello preventivo italiano. L'introduzione dell'IA ad alto rischio richiede un rigido rispetto delle scansioni procedimentali fissate dalla legge. L'obbligo di coinvolgimento dell'RLS poggia su un solido quadro normativo integrato: Art. 50, comma 1, lett. b), D.Lgs. n. 81/2008 sancisce che l'RLS «è consultato preventivamente e tempestivamente in ordine alla valutazione dei rischi, alla individuazione, programmazione, realizzazione e verifica della prevenzione nella azienda o unità produttiva», ponendo un focus specifico sull'«introduzione di nuove tecnologie»; l'Art. 26, par. 1, Regolamento (UE) 2024/1689 stabilisce che il *deployer* deve informare i lavoratori e i loro

ISSN 3035-4846

rappresentanti prima di mettere in servizio o utilizzare un sistema di IA ad alto rischio.

Nell'ordinamento italiano, la nozione di "informativa ai rappresentanti" deve coordinarsi con l'istituto della consultazione preventiva tenuto conto che un'informativa calata dall'alto a cose fatte non integrerebbe l'adempimento di cui all'art. 50 D.Lgs. n. 81/2008. Per soddisfare il requisito della "preventività e tempestività", la giurisprudenza[4] e la prassi[5] interpretativa concordano sulla necessità di avviare il procedimento di consultazione con un preavviso di almeno 30 giorni rispetto alla data di formale messa in funzione dell'algoritmo. Il datore di lavoro deve trasmettere all'RLS una documentazione analitica redatta in linguaggio chiaro e non esclusivamente tecnico, comprensiva di descrizione sintetica del funzionamento dell'IA, dei parametri di addestramento e della tipologia di dati processati, finalità d'uso e perimetro dei divieti (es. esplicita indicazione che il sistema non adotterà decisioni automatiche vincolanti sulla vita lavorativa o sull'idoneità sanitaria), bozza della sezione speciale del DVR e schema del protocollo di sorveglianza funzionale, diritti riconosciuti al lavoratore (accesso ai dati, richiesta di riesame umano, canale di segnalazione errori).

L'RLS ha il diritto formale di formulare osservazioni e proposte integrative ed il datore di lavoro è tenuto a riscontrare le osservazioni dell'RLS con motivazione congrua. L'intero iter deve trasfondersi in un verbale di consultazione, la cui assenza costituisce uno dei profili di censura primari in sede di ispezione da parte degli organi di vigilanza (INL e ASL).

4. Il raccordo con il medico competente: la riserva di funzione e il confine dell'art. 41 D.Lgs. n. 81/2008

L'interazione tra algoritmi di valutazione e sorveglianza sanitaria rappresenta uno dei punti più delicati dell'intero impianto normativo. In questa materia vige un limite invalicabile: la distinzione concettuale e giuridica tra valutazione di performance e giudizio medico-legale di idoneità.

L'output del sistema di IA costituisce esclusivamente una misurazione tecnico-operativa della prestazione (tempi di esecuzione, aderenza alle istruzioni operative, tasso di errore). Al contrario, il giudizio di idoneità alla mansione specifica di cui all'art. 41 del D.Lgs. n. 81/2008 è un atto medico-legale tipico, ad efficacia vincolante, riservato in via esclusiva ed inderogabile alla persona del medico competente.

[4] Cassazione Penale, Sez. IV, n. 48286/2017: La Suprema Corte ha ribadito la centralità e la non delegabilità sostanziale dei momenti partecipativi previsti dall'art. 50 D.Lgs. n. 81/2008. La consultazione non può ridursi a una mera "firma per presa visione" o comunicazione simulata ad assetti già definiti, ma deve garantire una reale interlocuzione preventiva. Se il tempo concesso all'RLS non permette l'analisi critica della complessità aziendale (a maggior ragione di un algoritmo ad alto rischio), l'obbligo di consultazione si considera omesso, integrando la contravvenzione sanzionata dal D.Lgs. 81/2008.

[5] La prassi operativa applica per analogia il termine di 30 giorni mutuandolo da due riferimenti normativi chiave: Art. 29, comma 3, D.Lgs. 81/2008: In caso di modifiche del processo produttivo o dell'organizzazione del lavoro (come l'introduzione di un sistema di IA ad alto rischio), la rielaborazione del DVR deve avvenire nel termine perentorio di 30 giorni; Art. 4, Legge 300/1970 i protocolli d'informazione e consultazione sindacale prevedono termini di preavviso informativo, di norma non inferiori a 30 giorni.

Tale giudizio scaturisce da un'esaminazione clinica, dall'anamnesi personale, dalla conoscenza diretta dei luoghi di lavoro e dalla valutazione delle condizioni psico-fisiche generali del lavoratore.

È tassativamente vietato al datore di lavoro utilizzare l'output dell'IA per sospendere, demansionare o trasferire un lavoratore adducendo presunte inidoneità fisiche o cognitive rilevate dall'algoritmo, sostituire la visita medica con l'elaborazione di indici statistici di rischio individuale generati dal software. Nel rispetto della riserva di funzione, l'IA può fornire elementi informativi indiretti di utilità per la prevenzione sanitaria.

A tal fine, prima della messa in funzione del sistema, il Datore di Lavoro, l'RSPP e il medico competente devono sottoscrivere un "Protocollo di raccordo", allegato al DVR, che disciplini flussi aggregati, vale a dire report anonimi e aggregati sulle deviazioni prestazionali per valutare l'insorgenza di fattori di rischio ergonomico o psicosociale nella mansione (art. 25, comma 1, lett. a, D.Lgs. 81/08), nonché segnalazione di anomalie individuali. In questo caso, il responsabile della sorveglianza funzionale, dinanzi a cadute repentine e anomale nelle prestazioni di un singolo lavoratore, limita l'azione alla segnalazione per l'attivazione di una visita medica straordinaria su richiesta o mirata. L'algoritmo attiva unicamente l'allerta clinica; la decisione sulla salute rimane un atto umano e professionale del medico.

5. La sorveglianza funzionale e la nuova disciplina dell'AI Literacy dopo il Digital Omnibus

L'*AI Act* e i successivi interventi correttivi europei riconoscono nella supervisione umana il baluardo fondamentale contro i rischi dell'automazione. L'art. 14, par. 4, e l'art. 26 dell'*AI Act* impongono al *deployer* di assegnare la sorveglianza umana a persone fisiche dotate della competenza, della formazione e dell'autorità necessarie per comprendere i limiti del sistema, intercettare le anomalie e interrompere il processo in caso di necessità. Sul piano dell'organizzazione aziendale, la sorveglianza funzionale non richiede la creazione di nuove figure apicali o contrattuali, bensì l'attribuzione formale di compiti di supervisione agli utilizzatori diretti o ai preposti debitamente formati.

Il modello operativo deve prevedere la costante facoltà per l'operatore di invalidare o correggere l'output algoritmico (*human-in-the-loop*), l'obbligo di registrazione delle anomalie riscontrate in un registro tracciabile, l'attivazione di canali diretti di segnalazione verso l'RSPP, la funzione HR e i servizi IT. Un elemento di rilevante impatto esegetico riguarda la riformulazione dell'art. 4 del Regolamento (UE) 2024/1689 operata dall'art. 1 del Regolamento (UE) 2026/1744 (*Digital* Omnibus). Nella versione originaria dell'AI Act, la norma imponeva a fornitori e deployer di «garantire un livello sufficiente di alfabetizzazione sull'IA» del proprio personale, configurando una potenziale obbligazione di risultato di

ISSN 3035-4846

difficile dimostrazione formale.

A seguito della novella introdotta dal Digital Omnibus, la formulazione è stata convertita in un'obbligazione di mezzi coordinata e flessibile: le organizzazioni sono tenute ad «adottare misure adeguate a sostenere lo sviluppo e il miglioramento dell'alfabetizzazione sull'IA del personale», tenendo conto delle loro conoscenze tecniche, della loro esperienza, della loro formazione e del contesto in cui i sistemi di IA devono essere utilizzati. Tale obbligo, operativo ed esigibile già dal 2 febbraio 2025, si integra virtuosamente con il sistema formativo del D.Lgs. n. 81/2008 (artt. 36 e 37).

Il datore di lavoro soddisfa la c.d. AI Literacy erogando moduli formativi mirati che forniscano agli operativi la comprensione della logica di funzionamento del modello e dei suoi limiti declarati dal costruttore, la capacità di rilevare allucinazioni, errori di classificazione e bias e, infine, la conoscenza dei protocolli di protezione dei dati personali e dei canali di segnalazione del rischio.

6. Profili sanzionatori, responsabilità 231 e quadro della compliance integrata

Il quadro di tutele s'arricchisce con il coordinamento della Legge 23 settembre 2025, n. 132[6] e dei successivi decreti legislativi attuativi approvati dal Consiglio dei Ministri il 4 agosto 2026[7], i quali definiscono l'architettura sanzionatoria nazionale e le Autorità competenti per la vigilanza (AgID e ACN). Sotto il profilo della responsabilità amministrativa degli enti (D.Lgs. 8 giugno 2001, n. 231)[8], l'integrazione dei reati informatici e dei delitti commessi mediante sistemi di IA (nuovo art. 25-vicies D.Lgs. 231/01) impone alle imprese di aggiornare i propri Modelli di Organizzazione e Gestione (MOG).

L'efficacia esimente del MOG 231 richiede che l'Organismo di Vigilanza (OdV) sia dotato di adeguate competenze in materia di sorveglianza algoritmica e che il DVR, nella sua Sezione IA, sia coordinato con i protocolli di prevenzione dei reati 231 e con la disciplina in materia di salute e sicurezza (art. 30 D.Lgs. 81/08).

L'introduzione nel catalogo dei reati-presupposto del nuovo art. 25-vicies del D.Lgs. 231/2001, preposto a sanzionare le illecite condotte informatiche e le fattispecie criminose realizzate mediante l'impiego di sistemi di Intelligenza Artificiale, impone una ridefinizione della struttura formale e sostanziale dei Modelli di Organizzazione, Gestione e Controllo. La ratio punitiva è rivolta nei confronti del deployer che abbia omesso o colposamente trascurato il governo funzionale.

[6] Legge 23 settembre 2025, n. 132, Disposizioni in materia di intelligenza artificiale, in G.U. n. 224 del 25 settembre 2025.

[7] Decreti Legislativi di attuazione e adeguamento della disciplina nazionale all'AI Act, approvati in via definitiva dal Consiglio dei Ministri il 4 agosto 2026.

[8] D.Lgs. 8 giugno 2001, n. 231, Disciplina della responsabilità' amministrativa delle persone giuridiche, delle società e degli enti privi di personalità giuridica, in G.U. n. 140 del 19 giugno 2001.

In tale prospettiva, l'efficacia esimente del MOG ai sensi dell'art. 6 del D.Lgs. 231/2001 non si soddisfa mediante la mera giustapposizione di protocolli cartacei o formali declaratorie di principio. Essa presuppone, invero, una compliance integrata e dinamica, incardinata su tre direttrici imprescindibili: in primo luogo, la competenza tecnica e la vigilanza algoritmica dell'OdV, dotato, direttamente o tramite ad hoc figure di supporto specialistico, di adeguate competenze in materia di audit algoritmico e tracciamento delle decisioni automatizzate (explainability e human oversight), onde garantire un'effettiva capacità di monitoraggio e di intercettazione dei rischi d'impresa legati all'autonomia operativa del software.

In secondo luogo, la sinergia strutturale tra DVR-IA e MOG 231: la Sezione del Documento di Valutazione dei Rischi dedicata all'Intelligenza Artificiale non costituisce un adempimento disarticolato rispetto alla prevenzione dei reati, ma assurge a presupposto logico-giuridico della mappatura dei rischi 231. Gli indicatori di anomalia della macchina (da bias discriminatori a falle di cybersecurity o deviazioni degli output) impongono una mappatura congiunta delle aree di vulnerabilità.

Da ultimo, il coordinamento con il sistema di prevenzione aziendale (art. 30 D.Lgs. 81/08) laddove l'architettura organizzativa esimente trova la sua naturale saldatura con l'art. 30 del D.Lgs. 81/2008. Ne consegue che l'incolumità psicofisica dei lavoratori e la sicurezza dei processi produttivi devono essere tutelate attraverso flussi informativi bidirezionali e costanti tra il Servizio di Prevenzione e Protezione (RSPP), il Medico Competente e l'Organismo di Vigilanza, realizzando una visione olistica del rischio d'impresa nell'era della transizione digitale.

7. Conclusioni

La portata dirompente delle novelle legislative europee e nazionali impone alle organizzazioni aziendali l'urgente superamento di un approccio meramente formale, sollecitando l'effettiva e tempestiva implementazione dei nuovi assetti regolatori nei processi di governance interna.

In questo mutato scenario, l'adempimento prescrittivo non può disgiungersi da un solido investimento nell'alfabetizzazione algoritmica (AI Literacy) e da un rigoroso principio di tracciabilità di ogni intervento operativo, procedimentale e valutativo posto in essere dall'impresa.

La corretta tenuta dei log, la documentazione dell'attività di human oversight e la formalizzazione dei passaggi partecipativi e sanitari assurgono a presupposti probatori ineludibili. Sarà infatti proprio sulla tenuta di tali garanzie procedurali e sostanziali che si concentrerà l'attività di verifica e controllo da parte degli organi ispettivi competenti, dalla cui adeguatezza dipenderà l'esito del nascente contenzioso giuslavoristico, amministrativo e penale legato all'impiego dell'Intelligenza Artificiale nei luoghi di lavoro.

ISSN 3035-4846