Guida al Lavoro

Il Punto - 23 ottobre 2025

L'intelligenza artificiale entra (davvero) in fabbrica e in ufficio

Sommario

Speciali Il Punto

L'intelligenza artificiale entra (davvero) in fabbrica e in ufficio

di Area Innovazione e AI – StanchiStudioLegale & Partners
N. 40 - 23 ottobre 2025

Come cambiano le regole per le imprese tra AI Act, GDPR, L.132/2025 e Statuto dei Lavoratori

Norme, prassi e responsabilità per chi guida le imprese nell'adozione dell'intelligenza artificiale nel lavoro. Cosa può fare il datore di lavoro, cosa non può fare, e come governare la complessità. In cui il termine veramente descrittivo è l'ultimo. Con l'articolo pubblicato sul numero precedente abbiamo aperto questa analisi per temi di alcune parti dell'AI Act, con il dichiarato intento di verificare alcune perplessità da un lato e di analizzare la complessità, nei limiti consentiti da questo mezzo di comunicazione, che questa tornata di normative di preteso governo tecnologico (ma indiscutibilmente burocratizzanti) hanno scaricato su imprese e cittadini. Il rapporto di lavoro è certamente una delle scene, cruciale per diritti e libertà ma anche cruciale per la produttività economica delle imprese, in cui l'elefante entra in cristalleria.
Il paradosso è che per governare le regole che vorrebbero governare la tecnologia (di cui pochi sanno qualcosa e tutti sappiamo pochissimo rispetto all'evoluzione) serve certamente l'intelligenza artificiale! Con buona pace di quell'intelligenza umana abile a semplificare processi complessi per renderli gestibili ad un essere con limitate abilità (la ruota era una soluzione semplice a problemi più complessi, ma oggi come ci è capitato di scrivere altrove sembrano tutti pensare che servano ruote quadrate).

GLI AUTORI

Riccardo Perlusz è stato dirigente in una multinazionale informatica, ricoprendo ruoli di rilievo sia sino alla direzione dei servizi di protezione aziendale all'interno dell'ufficio legale dell'azienda. Esperto in innovazione tecnologica, sicurezza aziendale e informatica giuridica, è anche relatore presso università e membro fondatore del Comitato Scientifico AIIAD 2024

Chiara Ciccia Romito Avvocata, PhD Lavoro Sviluppo e Innovazione, Università degli studi di Modena e Reggio Emilia

Andrea Stanchi Avvocato in Milano, esperto di diritto del lavoro, della privacy e dell'innovazione tecnologica

GPT5 Pro ed Explurimis - L'Ai - in soluzioni rigorosamente riservate allo Studio legale - collabora con gli Autori, in questo caso per editing, tabelle, ricerche giurisprudenziali. L'orchestrazione è sempre degli Autori cosiccome la responsabilità di ogni eventuale errore.

Speciali Il Punto

Il nuovo ecosistema normativo dell'intelligenza artificiale

di a cura Area Innovazione e AI – StanchiStudioLegale & Partners
N. 40 - 23 ottobre 2025

Il datore di lavoro che introduce sistemi di intelligenza artificiale deve oggi confrontarsi con un insieme di fonti normative eterogenee - europee e nazionali - che si intersecano e spesso si sovrappongono

Con l'entrata in vigore della Legge n. 132/2025 (alla quale rinviamo per la definizione di AI) e dell'AI Act europeo, il rapporto tra impresa, tecnologia e lavoratore entra in una nuova fase di regolazione. La relazione tra tecnologia e diritti (fondamentali), che è stata delegata per oltre 50 anni a quelle due norme (un po' sottovalutate) dello Statuto dei Lavoratori scritte nell'art. 4 e poi nell'8 (norma ancora più moderna e illuminata del primo), passa ad una nuova fase, che fa sembrare l'esperienza del GDPR una gita in sup sul lago (un minimo di equilibrio era comunque richiesto).

DEFINIZIONI (LEGGE N. 132/2025)

Art. 2 - Definizioni

1. Ai fini della presente legge, si intendono per:

Sistema di intelligenza artificiale - Il sistema definito dall'articolo 3, punto 1), del regolamento (UE) 2024/168

cioè un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e 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

Dato - Qualsiasi rappresentazione digitale di atti, fatti o informazioni e qualsiasi raccolta di tali atti, fatti o informazioni, anche sotto forma di registrazione sonora, visiva o audiovisiva;

Modelli di intelligenza artificiale - I modelli definiti dall'articolo 3, punto 63), del regolamento (UE) 2024/1689

cioè modello di IA per finalita` generali , un modello di IA, anche laddove tale modello di IA sia addestrato con grandi quantità di dati utilizzando l'autosupervisione su larga scala, che sia caratterizzato una generalità significativa e sia in grado di svolgere con competenza un'ampia gamma di compiti distinti, indipendentemente dalle modalità con cui il modello e` immesso sul mercato, e che può essere integrato in una varietà` di sistemi o applicazioni a valle, ad eccezione dei modelli di IA utilizzati per attività` di ricerca, sviluppo o prototipazione prima di essere immessi sul mercato;

2. Per quanto non espressamente previsto, si rimanda alle definizioni di cui al regolamento (UE) 2024/1689.

Adesso si parla di Big Wave surfing, ma a Nazarè e con onde da record del mondo.
Il datore di lavoro che introduce sistemi di intelligenza artificiale deve oggi confrontarsi con un insieme di fonti normative eterogenee — europee e nazionali — che si intersecano e spesso si sovrappongono: GDPR, Data Act, Statuto dei Lavoratori, Testo Unico Sicurezza, modelli di compliance 231/2001, regole di cibersicurezza e ora la disciplina specifica dell'AI Act e della legge italiana di attuazione. Il fine comune è duplice: garantire innovazione responsabile e tutelare la dignità del lavoratore, per tentare di mantenere un equilibrio tra automazione, trasparenza e controllo umano.

IL NUOVO ECOSISTEMA NORMATIVO DELL'INTELLIGENZA ARTIFICIALE IN SINTESI

AI Act: dal **2 febbraio 2025** stop alle pratiche vietate; obblighi per i sistemi high-risk (tra cui HR tech e monitoraggio

dipendenti) in progressiva entrata in applicazione fino al **2026–2027**; sanzioni fino al **7% del fatturato globale**.

- **L. 132/2025 (Italia):** in vigore dal 10 ottobre 2025; detta principi, istituisce osservatorio lavoro, rinvia a decreti attuativi e impone trasparenza verso utenti/clienti, coordinandosi con l'AI Act.

- **GDPR:** resta la "spina dorsale" (basi giuridiche, DPIA, art. 22 ADM), ma l'accesso ex art. 15 è spesso inefficace in chiave difensiva del lavoratore; la giurisprudenza UE ne amplia la portata ma l'enforcement transfrontaliero è lento.

- **Data Act:** applicabile dal **12 settembre 2025**; impone diritti di accesso/portabilità ai **dati generati da prodotti/servizi connessi (IoT)**, con forte impatto su fabbriche, veicoli, wearables e smart facility.

- **Statuto dei Lavoratori:** artt. **4** (controlli a distanza), **8** (divieto di indagini sulle opinioni) e **15** (atti discriminatori) costituiscono i "guard-rail" tradizionali, oggi da leggere insieme ad AI Act, GDPR e Decreto Trasparenza (art. 1-bis d.lgs. 152/1997).

Il 2025 segna un punto di svolta per le imprese europee.
L'AI Act, approvato definitivamente nel giugno 2025, definisce un quadro armonizzato di regole per l'impiego dell'intelligenza artificiale, basato su una classificazione dei rischi (vietati, alto rischio, limitato, minimo) e su obblighi proporzionati alla criticità dei sistemi. Parallelamente, la Legge 132/2025 istituisce in Italia un sistema di coordinamento nazionale al fine di promuovere l'uso etico e produttivo dell'IA. La Legge prevede, altresì, l'istituzione di un Osservatorio presso il Ministero del Lavoro e delle Politiche Sociali per monitorarne l'impatto nel mondo del lavoro.

IN SINTESI

A queste norme si affiancano strumenti già noti, ma che necessitano di reinterpretazione alla luce dell'IA: il GDPR (soprattutto gli artt. 13, 14, 15 e 22 e il Considerando 71), il Data Act (Reg. UE 2023/2854, in vigore dal 2025), e il tradizionale Statuto dei Lavoratori, in particolare gli artt. 4, 8 e 15, oltre al D.lgs. 231/2001, al D.lgs. 81/2008 e alle misure di cybersicurezza. L'impresa deve governare la complessità attraverso un approccio integrato, orientato alla piena governance dei dati e dei processi decisionali automatizzati, oltre alla mera conformità.

Non si tratta più solo di adottare strumenti tecnologici, ma di gestire sistemi decisionali autonomi che incidono direttamente su selezione, valutazione, produttività e sicurezza. È una rete normativa "intrecciata", non una sequenza: l'impresa deve imparare a muoversi in un sistema dove la compliance non è più lineare, ma circolare e interdisciplinare.

Dalla conformità alla governance: un cambio di paradigma

La crescente integrazione tra processi umani e algoritmici determina un necessario cambiamento culturale. L'intelligenza artificiale si configura come attore organizzativo che incide sulla produttività, sulla gestione delle risorse umane, sulla sicurezza, sulla formazione e sulla valutazione delle performance. Il mutamento descritto impone al datore di lavoro di integrare le funzioni legale, HR, IT, sicurezza e compliance in un modello operativo unico: l'"AI Operating Model'. In questo schema, la tecnologia deve essere progettata, validata e monitorata in modo interdisciplinare per garantire che la logica automatizzata non si traduca in controllo o discriminazione, ma sviluppi umanamente quel potenziale di aumento della produttività di cui la nostra economia ha un bisogno indispensabile.

La governance dell'intelligenza artificiale implica una gestione organica del rischio algoritmico, che comprende ma supera la dimensione della tutela dei dati personali. In questo la prospettiva normativa è indubbiamente meno visionaria dello Statuto (che sceglieva già la via, semplificando la distinzione tra fare e non fare derivandola dai diritti).

Nell'AI Act si legge la contraddizione tra saper fare e voler fare, che sono due cose molto diverse. Il Legislatore Statutario sapeva che futuro voleva, ha immaginato una società, a prescindere dall'evoluzione. Il Legislatore AI Act, come quasi tutti i legislatori europei attuali non ha la più pallida idea di che società vuole (e forse può volere) e dell'evoluzione tecnologica, che di fatto è agita altrove e gli è estranea (anche per merito di politiche fideistiche in quello che abbiamo sempre considerato l'amico americano?). Ne ha paura e ora non sa cosa fare, ma vuole fare qualcosa: risk based policy.

Il tentativo è riprodurre quella "sovranità attraverso la burocrazia" che il GDPR aveva dato (con tecnologie profondamente diverse e in certo modo distribuite) l'illusione per un ventennio di poter fare (ed oggettivamente era riuscito a fare sino al cambio di paradigma tech). Una sorta di riciclone del romano "divide et impera": arbitrare con le regole di utilizzo tra i produttori di tecnologia e consumatori di dati extraeuropei[1].

Peccato che l'AI sia tutta un'altra tecnologia, globale, pervasiva, esponenziale (e quindi attraverso regole timorose e burocratiche sostanzialmente ingovernabile, cosa che è già palese in un mondo che ha ben capito la differenza e quindi rifiuta la burocrazia del vecchio continente, di fatto condannandolo all'oblio tecnologico ed al relativo digital divide[2]).

La sfida che l'Ai Act riversa sulle imprese europee è garantire accountability, auditabilità e spiegabilità dei sistemi, in modo da bilanciare il potere informativo del datore con i diritti del lavoratore. Il Garante per la protezione dei dati personali, ha ripetutamente[3] segnalato che l'adozione di sistemi predittivi o di analisi comportamentale in ambito lavorativo richiede una valutazione d'impatto integrata — non solo privacy ma anche etica, organizzativa e sindacale.

Il concetto chiave è passare da "compliance" a "governance algoritmica".

Ogni decisione automatizzata deve essere spiegabile, auditabile e supervisionata da persone competenti. Il datore di lavoro deve poter dimostrare che la scelta di adottare un sistema AI è coerente con finalità legittime, trasparenti e proporzionate.

Questa nuova fase, come vedremo, trasforma la funzione HR e quella legale in centri di gestione del rischio tecnologico. E qui la questione diventa ancora più complessa: quali competenze possono essere messe in gioco e quali capacità interdisciplinari sono realmente attivabili in funzioni che per anni hanno selezionato e formato competenze giuridiche spesso verticali e specialistiche? Di contro l'introduzione di un sistema AI non può più essere decisa solo dal reparto IT dove viceversa, difficilmente prevale una visione estesa del mondo digitale al punto di incrociare per qualche verso la dimensione legislativa o giuridica del prodotto informatico. Per essere pragmatici servirebbero comitati interfunzionali dove siedano Legal, HR, IT, Sicurezza e

Compliance 231 salvo poi scontrarsi con dinamiche aziendali mal governabili. Tuttavia la posta in gioco è indubbiamente alta, a giudicare dalle sanzioni previste dal Regolamento europeo.

Quale norma si applica all'uso dell'IA nel rapporto di lavoro?

L'interazione tra l'AI Act e il GDPR (artt. 13–14–15–22, Considerando 71) rappresenta uno dei punti più delicati del nuovo diritto dell'intelligenza artificiale. Entrambi i regolamenti condividono l'obiettivo di garantire la trasparenza e la responsabilità nell'uso dei dati e dei sistemi automatizzati, ma adottano logiche e strumenti differenti. L'AI Act disciplina la progettazione e l'utilizzo dei sistemi AI, mentre il GDPR tutela i diritti fondamentali delle persone fisiche rispetto al trattamento dei dati personali. Nel contesto lavorativo, queste due dimensioni si sovrappongono: ogni sistema di IA che utilizza dati dei dipendenti per decisioni o monitoraggi è soggetto a entrambi i regimi.

LA NORMATIVA DI RIFERIMENTO

• **AI Act (Reg. UE 2024/1689)** - Pubblicato in G.U.U.E. il 12 luglio 2024, in vigore dal 1° agosto 2024; divieti assoluti operativi dal 2 febbraio 2025; gran parte delle norme dal 2 agosto 2026; gli obblighi "pesanti" per i sistemi ad alto rischio (inclusi quelli di impiego e gestione del personale) entrano a regime entro agosto 2027. (EUR-Lex)

NOTA BENE - Punto chiave per l'impresa: il capitolo "proibiti" è già applicabile e il perimetro "alto rischio" in HR va progettato ora, non nel 2027.

• **Legge n. 132/2025** ("Disposizioni in materia di intelligenza artificiale") - Pubblicata in G.U. 8 ottobre 2025, con entrata in vigore il 10 ottobre 2025. Istituisce, tra l'altro, l'Osservatorio per l'IA nel mercato del lavoro e coordina i profili nazionali con l'AI Act.

• **Data Act (Reg. UE 2023/2854)** - Regola accesso e uso dei dati generati da prodotti connessi e servizi correlati (IoT), cloud switcing e interoperabilità. Applicazione dal 12 settembre 2025 con varie finestre per switching e smart contract safeguards. Impatto HR: se usate wearable/IoT o macchine che generano dati su performance e sicurezza, cambia la governance dei dati "non-personali" e misti. (Normattiva)

• **GDPR** - Resta l'architrave per i dati personali, con due pezzi cruciali nel lavoro algoritmico: (i) trasparenza e diritto di accesso (artt. 12 e 15); (ii) art. 22 su decisioni unicamente automatizzate (in combinata con il diritto del lavoro); valutazione di impatto (art. 35) e misure di sicurezza (art. 32). La Corte di Giustizia ha precisato che l'"accesso" comprende copia "dei dati", non (sempre) "dei documenti" ma deve essere effettivo; ha anche chiarito a chi siano stati comunicati i dati.

• **Statuto dei Lavoratori**

– **art. 4 (controlli a distanza):** ammette strumenti "per esigenze organizzative e produttive" ecc., previo accordo sindacale o autorizzazione ispettiva; si applica anche a strumenti digitali/IA che consentano controllo a distanza.

– art. 8 (divieto di indagini sulle opinioni): attenzione a profiling che inferenzia idee politiche, sindacali, convinzioni religiose.

– **art. 15 (atti discriminatori):** nullità più tutela risarcitoria/ristoratoria; oggi va letto insieme a D.lgs. 215/2003 (origine razziale/etnica), 216/2003 (religione, convinzioni, handicap, età, orientamento sessuale) e 198/2006 (pari opportunità).

• **Decreto Trasparenza** (d.lgs. 104/2022): introduce in D.lgs. 152/1997 l'art. 1-bis con obblighi informativi specifici quando si usano sistemi decisionali o di monitoraggio automatizzati che incidono su assunzione, gestione, cessazione, assegnazione compiti, sorveglianza e valutazione. Richieste informazioni su logica/funzionamento, categorie dati/parametri (inclusi meccanismi di valutazione), controlli e processi di correzione, accuratezza/robustezza/cybersecurity con metriche. La violazione non si sana con informative "vaghe". Perché è cruciale per l'impresa: i) copre anche fase preassuntiva; 2) è lex specialis nel contesto lavoro, in coerenza con art. 88 GDPR (misure più appropriate: cfr. Garante Privacy)

[1] In realtà, come scritto nella precedente puntata (v. Quando l'intelligenza diventa artificiale, le regole per il lavoro dell'avvocato in Guida al Lavoro n. 39/2025), il cambio di paradigma (specie con avvento di social e gig economy) ha sottratto, a un legislatore (anche economico) disattento, "l'oro del regno" (i dati). Il fondamento del nuovo paradigma economico-finanziario. Non parliamo solo di tech o lavoro, ma di ascesa o declino economico di intere società. Come abbiamo scritto in epoche non sospette molti anni fa: il rischio è essere i nuovi INCA. Illuminatissimi, sino all'estinzione.

[2] La repentina virata con l'eliminazione degli Executive Orders di Biden da parte della nuova presidenza e il dibattito anche molto critico in letteratura specialistica d'oltre oceano e non solo ne sono chiara rappresentazione.

[3] Cfr. per tutti, Parere 477 del 2 agosto 2024 – Doc. web n. 10043532; Doc. web n. 10019984. provv. n. 234 del 10.06.2021 – Doc web n. 9675440; provv. n. 285 del 22.07.2021 – Doc web n. 9685994.

Speciali Il Punto

L'AI nei luoghi di lavoro, gli obblighi per le imprese

di Area Innovazione e AI – StanchiStudioLegale & Partners
N. 40 - 23 ottobre 2025

La regolazione del rapporto di lavoro tra controllo tecnologico e diritti dei lavoratori alla luce della normativa europea e nazionale, della giurisprudenza e dei provvedimenti del Garante privacy

L'AI Act visto dall'impresa

Dal 2 febbraio 2025 l'AI Act vieta: emotion recognition in luoghi di lavoro; social scoring; sfruttamento di vulnerabilità; sistemi di identificazione biometrica remota in tempo reale in spazi pubblici (salve strette eccezioni di polizia); biometric categorisation per tratti sensibili; untargeted scraping di immagini facciali per creare database.
Impatto per i datori di lavoro: nessun "sentiment scoring" su dipendenti/candidati; no face recognition in tempo reale in aree accessibili al pubblico (es. retail) per scopi di loss prevention; attenzione ai sistemi che deducono tratti sensibili. Le linee-guida della Commissione sui divieti hanno chiarito casistiche e confini applicativi (cfr. Strategia Digitale Europea).

PRATICHE VIETATE IN AZIENDA (GIÀ OPERATIVE)

Matrice operativa — quali sistemi si possono usare e come

Categoria AI Act	Esempi tipici in azienda (HR/Operations)	Stato in UE (lavoro)	Condizioni/Note
Vietati	Emotion recognition su dipendenti/candidati; biometric categorisation sensibile; scraping facciale massivo; face-ID live in spazi pubblici per loss prevention	Non utilizzabili (divieti immediati)	Solo eccezioni mediche/sicurezza; no retail privato con face-ID live
Alto rischio (Ann. III, p.4)	ATS con ranking CV; video-interview scoring; strumenti di scheduling/turni; performance/disciplinary scoring; allocazione bonus/premi	Ammessi con conformità rafforzata	Risk mgmt, data governance, documentazione, log, human oversight, accuratezza/robustezza/cyber; sorveglianza post-market; possibile registrazione EU DB
Rischio limitato	Chatbot HR informativi; sistemi di supporto con disclosure; generazione testi HR con etichettatura	Ammessi con trasparenza	Obbligo di informare l'utente che interagisce con AI; no decisione unicamente automatizzata
Rischio minimo	Automazioni interne non incidenti su persone; strumenti di office automation	Ammessi	Buone prassi: logging e security by design

ESEMPI DI TECNOLOGIE OFFERTE EXTRA-UE MA NON CONFORMI IN UE (CONTESTO LAVORO)

Nota pratica: molte offerte globali promuovono "emotion detection", "engagement scoring", "micro-expression analysis" o "fatigue detection" applicati a call center, telelavoro, magazzini. In Europa in ambito di lavoro tali sistemi rientrano nel divieto o, se non vietati per se, scivolano in alto rischio con requisiti proibitivi (es. biometric categorization/derivazioni di dati sensibili).

- Face recognition 'live' per retail/loss prevention (es. piattaforme come Facewatch in UK): non praticabile per datori privati in UE.

- Soluzioni di affective computing (Affectiva/Smart Eye) per engagement/fatica: vietate in ambito lavoro in UE.

- Video-interview con analisi facciale/voce (vecchie versioni di strumenti tipo HireVue): oggi non conformi.

- Servizi di face search/scraping (Clearview/PimEyes): sanzionati e incompatibili con GDPR e divieti AI Act.

Sistemi ad alto rischio nel lavoro

Il punto HR dell'AI Act è l'Allegato III (sistemi destinati a reclutamento, selezione, assegnazione compiti, valutazione prestazioni, promozioni/cessazioni ecc.), che li qualifica alto rischio, imponendo: risk management, data & data governance, documentazione tecnica, registrazione EU DB, sorveglianza post-market, human oversight sostanziale, accuratezza/robustezza e cybersecurity. Il testo e i documenti del Parlamento/Commissione fissano scadenze e cascate di standard (CEN-CENELEC JTC 21) che faranno da "manuale operativo" per le imprese. Per i deployers (gli utilizzatori, quindi normalmente la funzione che secondo la normativa l'azienda ricoprirebbe) scattano obblighi: uso conforme alle istruzioni, human oversight, logging, qualità dei dati, valutazione d'impatto sui diritti fondamentali (FRIA), quando richiesto a livello nazionale. Tempistiche: obblighi principali progressivamente entro 2026–2027 (cfr. Infra)[1]. Si tratta di oneri di conformità, organizzativi e procedurali di significativo impatto in termini di risorse impegnabili, soprattutto in considerazione dei profili di conoscenza e professionalità necessari.

Sanzioni e governance

Sanzioni fino a €35 mln o 7% del fatturato globale (per pratiche vietate); 3% per altre violazioni; 1% per informazioni fuorvianti. Coordinamento a livello UE tramite AI Office (GPAI) e autorità nazionali di vigilanza (EU AI Act) che a partire dal 10 Ottobre 2025 sono formalmente designate, congiuntamente ad altre Autorità, ai sensi dell'Art. 20 della L. 132/2025, alle attività di vigilanza e al controllo.

Le previsioni della legge n. 132/2025 per il lavoro

La L. 132/2025 ("Disposizioni e deleghe al Governo in materia di IA"), in vigore dal 10 ottobre 2025, introduce principi generali, misure di promozione, prime fattispecie penali, e soprattutto coordina l'ordinamento interno all'AI Act.
Focus lavoro (art. 11) - Al primo comma è stabilito il principio generale che l'utilizzo di tecnologia IA deve migliorare le condizioni lavorative tutelando integrità psico-fisica e dignità, accrescendo la qualità delle prestazioni lavorative e la produttività delle persone, in conformità al diritto dell'Unione europea e bilanciando in qualche modo diritti dei prestatori e interessi delle imprese. I limiti dell'utilizzo della tecnologia sono altrettanto chiari ed insuperabili: la tecnologia IA deve essere sicura, affidabile, trasparente e non può svolgersi in contrasto con la dignità umana né violare la riservatezza dei dati personali.
Vi è poi l'obbligo del datore di informare il lavoratore sull'uso di IA secondo l'art. 1-bis d.lgs. 152/1997 (Decreto Trasparenza). Previste garanzie antidiscriminatorie esplicite.

Il tema della IA nel "sistema lavoro" si presenta quindi particolarmente complesso e la prospettiva, chiara a tutti, è che l'introduzione di queste tecnologie aprirà un nuovo capitolo di lungo corso nel complesso sistema delle relazioni sindacali ed imprenditoriali. Per questo motivo il legislatore ha previsto con l'Art.12 della norma, la costituzione di un "Osservatorio sull'adozione di sistemi di intelligenza artificiale nel mondo del lavoro" presso il Ministero del Lavoro, con l'obiettivo di massimizzare i benefici derivanti dall'impiego di sistemi di IA in ambito lavorativo, contenendone i potenziali rischi, attraverso un vero e proprio lavoro di progettazione sociale fra le parti interessate e di monitoraggio dell'impatto sul mercato del lavoro della nuova tecnologia.
L'Osservatorio dovrà inoltre promuove la formazione dei lavoratori e dei datori di lavoro in materia di intelligenza artificiale, altro capitolo rilevantissimo per il corretto e soprattutto, consapevole uso di questa tecnologia, considerando l'esigenza di alfabetizzazione digitale che il comparto lavoro nel suo insieme dimostra di dover fare. La norma nazionale, tuttavia, vedrà un'attuazione graduale in quanto molte norme infatti richiederanno ulteriori decreti legislativi (già delegati al Governo dalla norma stessa) e quindi il quadro generale, la realtà operativa e quella sanzionatoria dipenderanno molto da questi atti.

Gli obblighi informativi (Artt. 13 e 15 GDPR)

La "parte del leone" negli obblighi previsionali e di informativa la fa il GDPR. Gli articoli 13, paragrafo 2, lettera f), e 15, paragrafo 1, lettera h) e il Considerando 71 del GDPR impongono al titolare del trattamento di fornire informazioni chiare sull'esistenza di processi decisionali automatizzati, sulle logiche utilizzate e sulle loro conseguenze per l'interessato. Gli obblighi impongono al titolare del trattamento di fornire all'interessato (leggi dipendente) informazioni chiare, complete e comprensibili circa le finalità, le basi giuridiche, le categorie di dati trattati, le logiche dei processi decisionali automatizzati e i diritti esercitabili. Nel caso di sistemi di IA, al focus in merito al dato e all'informazione che questo veicola nel merito di un processo automatizzato, si aggiunge l'onere informativo circa la componente algoritmica, ovvero dei meccanismi e delle logiche che rendono una inferenza autonoma rispetto alla procedura sino ad oggi semplicemente automatizzata. A questo si aggiunge l'informazione su come potenziali o possibili errori o pregiudizi vengano dall'algoritmo della funzione AI utilizzata, intercettati e corretti, ciò implica che il lavoratore debba essere informato non solo dell'esistenza del trattamento, ma anche della presenza di meccanismi automatizzati di valutazione o monitoraggio, delle metriche principali impiegate e delle misure adottate per ridurre gli errori o i bias. Il Considerando 60 del GDPR precisa che le informazioni devono consentire una comprensione effettiva e non meramente formale del trattamento, il che in tema di AI (per esperienza d'utilizzo, tutt'altro che prevedibile nelle soluzioni della blackbox) apre complessità non indifferenti. In ambito occupazionale, il Garante per la protezione dei dati personali ha più volte richiamato l'esigenza di evitare informative generiche. Il provvedimento n. 408 del 15 dicembre 2023 ha chiarito che, quando un algoritmo incide su assunzioni, premi o provvedimenti disciplinari, le informative devono includere la logica di funzionamento del modello, i parametri più rilevanti e la possibilità di intervento umano (il c.d. man in the loop[2]). Qui il tema rilevante torna. Vi è un onere generale di elevare il livello di conoscenza e di padronanza della tecnologia digitale, in particolar modo nel campo della IA affinché vi siano le condizioni utili a un reale ed effettivi uso adeguato e consapevole di strumenti che portano grandi vantaggi (efficienza, completezza, utilità) ma nello stesso tempo ampi rischi, maggiormente legati all'incapacità umana di usare ed interpretare la tecnologia, piuttosto che il contrario. Tali obblighi si inseriscono in un quadro in cui la sicurezza delle informazioni costituisce il presupposto tecnico e operativo per l'effettivo esercizio dei diritti riconosciuti. L'integrità dei dati assicura la coerenza tra i dati originari e quelli impiegati nei processi decisionali; la disponibilità dei sistemi consente l'esercizio dei diritti di accesso e rettifica; la riservatezza dei trattamenti tutela l'interessato da usi impropri o discriminatori delle informazioni.

Decisioni automatizzate e garanzie (art. 22 e considerando 71 GDPR)

L'articolo 22 del GDPR riconosce all'interessato il diritto di non essere sottoposto a decisioni fondate unicamente su trattamenti automatizzati di dati personali, comprese le attività di profilazione, qualora tali decisioni producano effetti giuridici o incidano in modo analogo sulla sua sfera personale.
La norma prevede eccezioni nei casi in cui il processo decisionale automatizzato sia necessario per l'esecuzione di un contratto, autorizzato dal diritto dell'Unione o dello Stato membro, oppure basato sul consenso esplicito dell'interessato. In tali ipotesi, il titolare deve garantire adeguate tutele, tra cui l'intervento umano, la possibilità di esprimere opinioni e di contestare la decisione.
Le Linee guida 2/2019 del Comitato Europeo per la Protezione dei Dati chiariscono che la nozione di "necessità contrattuale" non coincide con una lettura letterale delle clausole, ma implica la verifica della reale indispensabilità del trattamento rispetto all'esecuzione del contratto. Nel contesto lavorativo, rientrano in questa categoria le decisioni di assunzione, valutazione, promozione, licenziamento e attribuzione di premi o turni. Il Considerando 71 specifica che tali trattamenti devono essere accompagnati da garanzie adeguate: diritto di intervento umano, di esprimere la propria opinione e di contestare la decisione. Questo principio, se combinato con l'AI Act, impone che i sistemi di alto rischio adottati nei processi HR garantiscano meccanismi di oversight effettivo e documentabile. La supervisione umana deve essere reale, non simbolica: il lavoratore deve sapere chi può modificare o annullare una decisione automatizzata e in quali tempi.

L'integrazione con l'AI Act: trasparenza e spiegabilità

L'AI Act, negli articoli 13 e 14, introduce obblighi specifici di trasparenza e fornitura di informazioni agli utenti e agli interessati. Tali obblighi si sommano, ma non si sovrappongono, a quelli del GDPR. In particolare, l'articolo 13 dell'AI Act prevede che gli utilizzatori di sistemi di alto rischio debbano garantire che il personale umano comprenda le capacità e i limiti del sistema, mentre l'articolo 14 impone l'adozione di misure per assicurare la supervisione umana durante tutto il ciclo di vita del sistema. In questa prospettiva, l'impresa deve coordinare i propri adempimenti: l'informativa ai sensi del GDPR articoli 13 e 14, la documentazione tecnica richiesta dall'AI Act e le procedure interne di audit e monitoraggio. Un'unica governance integrata consente di evitare duplicazioni e garantire coerenza tra trasparenza normativa e reale accountability operativa.
Non possiamo che sottolineare due aspetti rilevanti in merito all'adempimento di questi oneri per il datore di lavoro. Il primo punto è relativo alla spiegabilità dell'algoritmo, parte funzionale di un processo, laddove i prodotti utilizzati derivino da servizi digitali erogati dai fornitori terzi, modalità attuativa delle tecnologie IA praticamente universale. In questo caso può diventare complesso ottenere le informazioni necessarie e spesso se ne ottengono solo una parte in ragione di regole di riservatezza alzate dai fornitori stessi. Talché diventa indispensabile una valutazione attenta, a partire dai contratti di fornitura, laddove si è in ambito di infrastrutture tecnologiche che si appoggiano su servizi applicativi esterni all'interno di processi interni. Il secondo punto è relativo al monitoraggio e ad eventuali audit che per condizioni analoghe, debbono essere ripensati e organizzati opportunamente.

Statuto dei Lavoratori (artt. 4, 8, 15), prassi Garante e giurisprudenza 2023–2025

Nella prospettiva dell'impresa (e del datore di Lavoro in genere), lo Statuto dei Lavoratori, pur risalente al 1970, conserva un ruolo centrale nella regolazione del rapporto tra controllo tecnologico e diritti dei

lavoratori. L'introduzione di sistemi di intelligenza artificiale e di analisi automatizzata delle prestazioni richiede un accenno alla lettura sistematica degli articoli 4, 8 e 15 alla luce dell'evoluzione tecnologica e delle più recenti pronunce della giurisprudenza e del Garante per la protezione dei dati personali.

Strumenti di controllo a distanza e AI come 'strumento di lavoro' (art. 4 St. Lav.)

L'articolo 4 dello Statuto dei Lavoratori rimane il fulcro del controllo datoriale.
L'introduzione di sistemi di intelligenza artificiale non elimina, ma anzi amplifica il rischio di controllo indiretto (perchè occorre ricordare che quello diretto sulle modalità della prestazione era ed è vietato, divenuto principio dell'Ordinamento dopo la modifica del 2015, per giurisprudenza granitica[3]) della persona del lavoratore. L'articolo 4 dello Statuto distingue (comma 1) tra strumenti di controllo a distanza, soggetti a previo accordo sindacale o autorizzazione dell'Ispettorato Nazionale del Lavoro (con le moderazioni dell'accordo/autorizzazione a livello nazionale laddove imprese distribuite sul territorio), e strumenti "di Lavoro" che servono al lavoratore per rendere la prestazione lavorativa o servono alla sicurezza del lavoro. Quest'ultima nozione è stata sempre interpretata restrittivamente dalla giurisprudenza e dal Garante (sostanzialmente in modo abrogante). Nel contesto dell'intelligenza artificiale, questa distinzione diventa estremamente complessa: un software di pianificazione turni basato su AI o un sistema di analisi produttiva può contemporaneamente costituire strumento di organizzazione e di controllo[4]. Quindi di fatto ogni strumento di AI, salvo che il nostro Legislatore prenda auspicabili strade specificative distinguendo almeno sui temi sicurezza (intendendosi sia quella cyber, che oggi ha apparati di norme imperative importanti, che è inutile passino da accordo sindacale o autorizzazione: sono obbligatori; sia sicurezza sul Lavoro: strumenti che controllano ma per il fine della sicurezza della persona potrebbero ben essere identificati secondo albi magari tenuti ed aggiornati dal Ministero ed evitare burocratizzazioni inutili ed inefficienti, ma ...).
Va ricordato che la giurisprudenza recente[5] ha chiarito che anche i sistemi digitali apparentemente neutrali rientrano nel perimetro dell'art. 4 se generano effetti di monitoraggio diretto o indiretto sulle prestazioni dei lavoratori. Il Garante, nel provvedimento di parere sull'AI (n. 477/2024), ha ribadito che le piattaforme di gestione HR e i software di valutazione automatizzata richiedono, oltre alla DPIA, una preventiva valutazione congiunta tra datore, DPO e rappresentanze sindacali, poiché possono comportare un controllo a distanza non autorizzato. E con i vari provvedimenti 2022–2024, ha precisato che anche il tracciamento di metriche di produttività e presenza rientra nell'ambito dell'art. 4.
La supervisione algoritmica non può essere surrogata da algoritmi "black box": il datore resta titolare e responsabile[6].
L'art. 4, comma 2, consente l'uso dei dati raccolti dagli strumenti di lavoro solo nel rispetto delle garanzie procedurali previste e dell'informativa ai lavoratori. Pertanto, l'AI utilizzata come supporto all'attività (ad esempio, strumenti di assistenza decisionale o di manutenzione predittiva) deve essere di fatto sempre accompagnata da informative specifiche (e da un accordo sindacale se i dati generano un controllo sistematico o profilato: cfr, infra per le considerazioni sulla relazione tra le norme).

Divieto di indagini sulle opinioni e limiti informativi dei sistemi AI (art. 8 St. Lav.)

L'articolo 8 dello Statuto dei Lavoratori vieta al datore di lavoro di effettuare indagini, anche tramite terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale. Con l'avvento dei sistemi di AI, questo divieto si estende alle analisi

inferenziali basate su dati comportamentali, linguistici o di social listening. In altre parole, anche se l'algoritmo non raccoglie direttamente opinioni, può inferirle da pattern testuali, cronologici o relazionali, violando lo spirito dell'art. 8.
Il Garante[7] ha ritenuto illecito l'uso di software di analisi del linguaggio nei colloqui di selezione che valutavano tratti di personalità e predisposizione all'autorità, in quanto idonei a rivelare opinioni o caratteristiche personali non pertinenti. Sistemi dichiaratamente di well being del dipendente (ve ne sono diversi sul mercato, anche nelle principali suite di strumenti) sono sistemi che se non adeguatamente configurati si schiantano sul tema dei controlli vietati dal combinato di art. 4 e art. 8. È un limite sostanziale all'uso di strumenti di emotion AI o affective computing, spesso venduti come indicatori di "engagement" ma vietati in Europa. Il principio di pertinenza e non eccedenza si applica dunque in modo rafforzato ai sistemi di AI: l'impresa deve configurare gli algoritmi in modo che trattino solo informazioni strettamente necessarie alla funzione lavorativa.
La giurisprudenza conferma questa linea: la Corte di Cassazione, con sentenza n. 25731 del 2021[8], ha dichiarato illegittimo l'utilizzo di dati tratti da analisi comportamentali su chat aziendali per fini disciplinari, ritenendo che essi travalicassero il perimetro dell'attività professionale e sfociassero in un controllo vietato ex art. 8.

Divieto di atti discriminatori e valutazioni algoritmiche (art. 15 St. Lav.)

L'articolo 15 dello Statuto sancisce la nullità degli atti discriminatori e la tutela contro trattamenti differenziati per motivi di sesso, età, orientamento, razza o convinzioni. Nel contesto AI, ciò si traduce nell'obbligo di testare i sistemi per individuare bias o correlazioni spurie che possano produrre disparità di trattamento. Va inoltre posto un altro livello di attenzione che ancora una volta richiama il dato. Assunto che i sistemi IA si alimentano dei dati generati dai processi che li utilizzano e strutturano il loro modello di inferenza o decisione in base ai risultati del proprio processo, è di particolare rilevanza l'attenzione alla qualità del dato introdotto nel sistema, che altrimenti porta in degrado il sistema con conseguenze introduzione nel processo di elementi discriminanti o errati. Onere quindi nell'uso di queste tecnologie per ottenere reale conformità, è il processo di verifica delle modalità di acquisizione e trattamento dei dati utilizzati.
Il datore di lavoro deve documentare le verifiche effettuate e mantenere la tracciabilità delle decisioni automatizzate, in linea con i principi del Considerando 71 GDPR e con le clausole di fairness introdotte dall'AI Act. A queste valutazioni si sovrappongono anche quelle imposte dai D.lgs. 216 e 215/2003 e il 198/2006 (parità di genere). Anche questi si applicano alle decisioni algoritmiche; ricordando che il rito speciale antidiscriminatorio consente l'alleggerimento dell'onere probatorio anche per via statistiche (utile contro bias sistemici), la complessità della valutazione datoriale è evidente. Integrare questi strumenti con AI Act/Statuto è cruciale per prevenire impact discrimination in selezione e gestione HR, ecc.. Ma l'appesantimento per la funzione HR è tale da far dubitare dell'effettività (preventive) dello schema normativo risultante.

Gestione dei dati, responsabilità organizzativa e tutela della salute e sicurezza nei luoghi di lavoro

L'evoluzione dell'intelligenza artificiale nelle imprese si intreccia con un più ampio quadro normativo che coinvolge la gestione dei dati, la responsabilità organizzativa e la tutela della salute e sicurezza nei luoghi di lavoro. Il Data Act, la Legge 132/2025, il D.Lgs. 231/2001 e il D.Lgs. 81/2008 rappresentano i pilastri di una governance integrata che deve garantire, in chiave sistematica, trasparenza, tracciabilità e sicurezza tecnologica.

Il Data Act e la gestione dei dati generati dall'IA

Il Data Act (Regolamento UE 2023/2854) introduce regole uniformi per l'accesso e l'utilizzo dei dati generati da prodotti e servizi connessi, includendo anche i dati derivati dai sistemi di intelligenza artificiale. Il Data Act completa l'AI Act, garantendo alle imprese e ai lavoratori accesso e portabilità dei dati generati dai sistemi connessi.
Nel contesto aziendale, questo implica che i dati raccolti dai sensori, dai macchinari intelligenti o dai software di analisi predittiva devono essere accessibili in modo equo, sicuro e interoperabile. Per i datori di lavoro, il Data Act comporta nuovi ulteriori obblighi di governance: garantire che i dati contenenti informazioni personali dei lavoratori siano gestiti in conformità al GDPR e, allo stesso tempo, accessibili per fini produttivi in modo conforme alle regole di concorrenza e di proprietà intellettuale.
Un aspetto critico riguarda la distinzione tra 'dati di macchina' e 'dati personali'. In molti contesti industriali, le telemetrie dei macchinari possono riflettere indirettamente comportamenti dei lavoratori. La sovrapposizione tra questi ambiti richiede un approccio prudente: i dati tecnici vanno trattati come personali ogni volta che consentono, anche indirettamente, l'identificazione o la valutazione della prestazione di un individuo (pensate alle prestazioni della GIG Economy). Il datore di lavoro deve pertanto predisporre procedure di anonimizzazione o minimizzazione dei dati, documentate e verificabili. E forse si apre un tema (tutt'altro che secondario o semplice), che comincia a profilarsi nelle discussioni anche d'oltreoceano, sulla proprietà dei dati prodotti dai lavoratori[9]

Un quadro nazionale di raccordo, la Legge 132/2025

Come anticipato, la Legge 132/2025 costituisce il principale strumento di attuazione e coordinamento dell'AI Act in Italia. Essa istituisce l'Osservatorio nazionale sull'intelligenza artificiale presso il Ministero del Lavoro e introduce una serie di principi di etica, trasparenza e non discriminazione da applicare anche in ambito lavorativo. Inoltre, prevede la promozione di linee guida nazionali per l'uso sicuro dell'IA nei processi produttivi, formativi e gestionali, con particolare attenzione alle PMI e ai settori industriali ad alta automazione.
Dal punto di vista operativo, la legge impone al datore di lavoro di integrare la valutazione dell'impatto algoritmico nei processi di risk management aziendale. Questo significa che, accanto alla DPIA prevista dal GDPR e alla valutazione di conformità prevista dall'AI Act, occorre sviluppare una metodologia unificata che tenga conto anche dei rischi etici, reputazionali e organizzativi. La legge sottolinea inoltre la necessità di formazione del personale sull'uso consapevole dei sistemi di IA e la promozione di audit periodici sulla qualità dei dati.

Responsabilità organizzativa e modelli di compliance (D.Lgs. 231/2001)

Il D.Lgs. 231/2001, originariamente concepito per prevenire reati d'impresa, assume oggi un nuovo ruolo nella gestione dell'IA. L'adozione di sistemi algoritmici può infatti generare rischi di illecito legati a discriminazioni, violazioni della privacy, omissioni di vigilanza o lesioni dei diritti dei lavoratori. Bene precisare che la Lg. 132 ha introdotto le prime modifiche alle norme penali e ha dato delega al Governo per l'adeguamento delle fattispecie di reato in cui la tecnologia IA possa essere utilizzata per il perfezionamento di comportamenti illeciti. Non possiamo quindi che aspettarci che queste fattispecie arricchiscano il novero dei reati supposti della norma sulla responsabilità dell'impresa, e che per loro natura, siano effettivamente un rischio importante per la responsabilità datoriale e per l'obbligo di vigilanza che ne deriva. Per questo motivo,

i modelli organizzativi devono essere aggiornati includendo l'IA nel perimetro dei rischi e delle procedure di controllo interno. La L. 132/2025 prevede espressamente un ampliamento "algoritmico" dei reati inclusi.

L. 132/2025	Oggetto della delega / intervento normativo	Termine per l'adozione del decreto delegato
Art. 16 – "Delega al Governo in materia di dati, algoritmi e metodi matematici per l'addestramento di sistemi di intelligenza artificiale".	Regolamentazione organica di dati, algoritmi e metodi utilizzati per IA: definizione delle modalità, trasparenza, audit, responsabilità	**Entro 12 mesi** dalla data di entrata in vigore della legge.
Art. 24 – "Delega al Governo in materia di intelligenza artificiale".	Adeguamento della normativa nazionale al regolamento (UE) 2024/1689 (IA Act): settore bancario, finanziario, assicurativo, servizi di pagamento, etc.	**Entro 12 mesi** dalla data di entrata in vigore della legge.
Art. 20, comma 3 – "Il Governo è delegato ad adottare, entro dodici mesi dalla data di entrata in vigore della legge, uno o più decreti legislativi per adeguare e specificare la disciplina dei casi di realizzazione e di impiego illeciti di sistemi di intelligenza artificiale."	Definizione degli illeciti specifici di IA, sanzioni, responsabilità, coordinamento con codice penale, normative 231 applicabili	**Entro 12 mesi** dalla data di entrata in vigore della legge.

Per le imprese e per i rispettivi organismi di vigilanza ciò significa: ampliare la mappatura dei rischi al di là degli ambiti tradizionali (corruzione, frode, reati societari), considerare i nuovi scenari legati all'uso dell'intelligenza artificiale e dei dati, prevedere procedure dedicate, potenziare la formazione del personale e rinforzare le capacità dell'OdV. Parallelamente, l'entrata in vigore del Regolamento UE 2023/2854 (Data Act) introduce una dimensione ulteriore: la governance dei dati e della condivisione degli stessi assume rilievo come fattore di rischio 231, laddove l'utilizzo dei dati alimenta sistemi di IA o decisioni automatizzate aziendali. Con i decreti delegati che dovranno essere approvati entro il 2026, le imprese avranno una finestra relativa al recepimento; ma è consigliabile un'azione preventiva immediata sull'aggiornamento del modello 231 e dell'OdV, al fine di presidiare i nuovi rischi e consolidare la governance interna. La vigilanza sull'AI rientrerà nelle competenze dell'Organismo di Vigilanza (OdV), in coordinamento con Audit, DPO e RSPP. L'adozione di un "AI Risk Register" e di audit periodici potrebbe essere introdotto per documentare la diligenza richiesta dall'art. 6 D.Lgs. 231/2001.

Sicurezza, salute e impatto dei sistemi AI (D.Lgs. 81/2008)

Il Testo Unico sulla Sicurezza (D.Lgs. 81/2008) prevede un Allegato XXXIV, molto trascurato in tema di relazione tra rischi tecnologici e salute, che deve essere oggi reinterpretato alla luce dei nuovi rischi introdotti dall'automazione intelligente. È qui che si gioca il vero salto concettuale.
L'Allegato XXXIV, che definisce le informazioni e la formazione dei lavoratori in materia di sicurezza, diventa oggi la base per una nuova sicurezza algoritmica. Le imprese dovranno interpretarlo in chiave digitale:

- la "formazione sufficiente e adeguata" diventa formazione sull'uso consapevole dei sistemi AI, competenze minime di AI literacy per riconoscere errori, bias o falsi positivi;
- la valutazione dei rischi (DVR) dovrà includere rischi cognitivi e decisionali, legati a bias, opacità o dipendenza da modelli predittivi;

- la cooperazione tra datore, dirigenti e RSPP si estende alla figura del DPO e del Chief AI Officer o General Counsel tecnologico, che coordina le aree giuridiche, etiche e di sicurezza.

I sistemi AI possono incidere sul carico cognitivo, sulla sorveglianza continua e sulla gestione dei cobot (robot collaborativi), generando rischi psicosociali e fisici. Il datore di lavoro è quindi tenuto ad aggiornare il Documento di Valutazione dei Rischi (DVR) includendo le dimensioni legate all'interazione uomo-macchina e ai bias decisionali. La mancata formazione su tali aspetti potrebbe configurare violazione dell'art. 37 del TU 81/08 e responsabilità penale del datore per infortunio digitale. L'estensione logica è già riconosciuta da linee guida INAIL 2025 sulla digitalizzazione sicura e dalla proposta di "AI safety by training" della Commissione. In questa prospettiva, la sicurezza non è più solo fisica, ma cognitiva, informativa e algoritmica. L'INAIL e il Garante hanno raccomandato di considerare: (a) l'effetto della sorveglianza algoritmica sul benessere mentale; (b) i rischi di sostituzione decisionale automatica; (c) la necessità di formare il personale alla supervisione dei sistemi. In quest'ottica, la sicurezza sul lavoro non è più solo fisica ma anche digitale, e la prevenzione deve comprendere la trasparenza e la contestabilità delle decisioni dell'IA. La complessità degli oneri valutativi datoriali si viene quindi profilando in tutta la sua considerevolissima ampiezza.

---

[1] Es. Cfr. Standard & framework utili (anche per PMI):
- ISO/IEC 42001:2023 (AI Management System): impianto certificabile per governance, risk e controlli; ottimo "ponte" tra GDPR, AI Act e qualità. (ISO)
- NIST AI Risk Management Framework 1.0: pratico per mappare-misurare-gestire rischi e bias, con casi HR e supply-chain. (mccannfitzgerald.com)
- CEN-CENELEC JTC 21: in corso di sviluppo standard armonizzati a supporto dell'AI Act (beneficio: presunzione di conformità). (CEN-CENELEC)

[2] Il loop in cui l'human deve restare attore decidente è concettualmente basato sull'O(bserve)O(rient)D(ecide)A(ct) John_Boyd_(military_strategist), ma si focalizza sul ruolo del fattore umano in processi decisionali complessi (spesso tecnologici). L'OODA descrive il ciclo cognitivo naturale dell'essere umano; il "loop del man" o "human-in-the-loop" descrive il modo in cui quel ciclo interagisce con sistemi automatici o digitali.

[3] Cfr. Tar Lazio, 23 novembre 2022 n. 15644; Cass. 25372/2021.

[4] Cfr. es. Doc web n. 9823282.

[5] Informativa trasparente ex artt. 13 GDPR (con I vincoli di Considerando 71, art. 13 e 14 e 22) e art. 1-bis d.lgs. 152/1997. Ma poi vediamo infra anche i temi di interferenza con le valutazioni di sicurezza imposte dal TU 81/08.

[6] Post-market: logging, audit, gestione incidenti e riesame umano tracciabile.

[7] Cfr. M. Peruzzi, L'impatto dell'AI nella selezione del personale, https://www.lavorodirittieuropa.it/dottrina/principi-e-fonti/1660-l-impatto-dell-ia-nella-selezione-del-personale-negli-annunci-di-lavoro-mirati-a-filtrare-le-candidature-nella-determinazione-della-reputazione-della-persona-che-lavora-e-nell-assegnazione-dei-compiti; cfr. es. provv. 10 aprile 2025. Cfr. anche il provv 11 gennaio 2024 [doc. web n. 9983415]

[8] Ma v. anche Cass. 18168/23

[9] Cfr. es. documento di lavoro 149 dell'OIL: https://www.ilo.org/publications/navigating-workers-data-rights-digital-age

Speciali Il Punto

Adozione di sistema di intelligenza artificiale: la sequenza logico-sistematica delle valutazioni aziendali

di Area Innovazione e AI – StanchiStudioLegale & Partners
N. 40 - 23 ottobre 2025

Il datore di lavoro dovrebbe poter produrre un documento unico, denominato 'Fascicolo integrato AI–HR', che rappresenta la prova documentale dell'approccio sistemico dell'impresa e può essere utilizzato in sede ispettiva, giudiziale o di certificazione

L'adozione di un sistema di intelligenza artificiale che incida sull'attività o sulle decisioni relative ai lavoratori richiede, quindi, una sequenza logica e coerente di valutazioni preventive. Questa sequenza deve rispettare l'ordine di priorità tra le normative settoriali e garantire la coerenza dell'intervento aziendale, evitando duplicazioni o omissioni. La logica è quella della 'compliance integrata': un approccio che unisce privacy, sicurezza, etica, responsabilità e diritto del lavoro.

La gerarchia normativa e la logica di prevalenza

Nel sistema giuridico, le norme europee direttamente applicabili prevalgono sulle disposizioni nazionali incompatibili. Di conseguenza, l'AI Act e il GDPR costituiscono la cornice primaria di riferimento per l'utilizzo dei sistemi di intelligenza artificiale. Lo Statuto dei Lavoratori, il Data Act, la legge 132/2025 e le discipline interne (231 e 81/08) si integrano come livelli attuativi e specializzazioni settoriali.

L'ORDINE DI PRIORITÀ LOGICO

1. AI Act e L. 132/2025 – definisce la liceità e le condizioni tecniche di utilizzo dei sistemi AI (divieti, classificazioni, obblighi di supervisione e trasparenza).

2. GDPR – disciplina il trattamento dei dati personali, garantendo i diritti fondamentali degli interessati (artt. 13, 14, 15, 22, Cons. 71).

3. Statuto dei Lavoratori – integra la base giuridica del trattamento, tutelando la dignità e la riservatezza del lavoratore (artt. 4, 8, 15 e normative sulla discriminazione dei decreti di matrice europea richiamati sopra).

4. Data Act – regola la gestione dei dati e la governance dei sistemi digitali.

5. D.Lgs. 81/2008 – assicura la tutela della salute e della sicurezza, includendo oggi anche i rischi psicosociali e digitali.).

6. D.Lgs. 231/2001 – impone una valutazione di coordinamento che si riverbera sull'adozione di modelli organizzativi di prevenzione e controllo (passare dalla fine per costruire le regole di dettaglio della azione aziendale in combinato con quell'informativa necessitata dalle norme richiamate sopra.

La sequenza operativa di valutazione

La corretta applicazione delle norme richiede un percorso sequenziale articolato in fasi. Ogni fase deve essere documentata e integrata nelle politiche aziendali di governance tecnologica:
1. Analisi di ammissibilità (AI Act L. 132/2025) – Identificare la categoria del sistema AI (vietato, alto rischio, limitato, minimo) e verificare la possibilità giuridica del suo utilizzo. I sistemi vietati non possono essere adottati; per quelli ad alto rischio, scatta l'obbligo di valutazione di conformità e sorveglianza post-market.

2. Valutazione di impatto sui dati (GDPR) – Eseguire la DPIA ai sensi dell'art. 35 GDPR, considerando non solo la sicurezza ma anche la spiegabilità e la non discriminazione. La DPIA deve integrarsi con il fascicolo tecnico richiesto dall'AI Act.
3. Verifica sindacale e autorizzativa (Statuto dei Lavoratori) – Valutare se il sistema comporta un controllo diretto o indiretto sull'attività dei lavoratori (difficile pensare, allo stato della normative e dell'interpretazione sistemi che riguardano il Lavoro che non le implichino). In tal caso, è obbligatorio un accordo sindacale o l'autorizzazione dell'Ispettorato Nazionale del Lavoro, ai sensi dell'art. 4, comma 1. La mancata autorizzazione comporta l'inutilizzabilità dei dati ai fini disciplinari, l'illiceità del trattamento e corollari conseguenti, ivi inclusi a seconda dei casi i rischi penali.
4. Revisione organizzativa e di responsabilità (D.Lgs. 231/2001) – Integrare l'IA, per I profili di rilevo, nel modello organizzativo e aggiornare i protocolli di vigilanza e le deleghe.
5. Valutazione dei rischi per la salute (D.Lgs. 81/2008) – Aggiornare il DVR includendo l'impatto cognitivo e psicosociale della supervisione algoritmica. Coinvolgere RSPP e medico competente nelle fasi di progettazione e monitoraggio.
6. Comunicazione e formazione (L. 132/2025, GDPR art. 13, Decreto Trasparenza, Art. 4 St. Lav) – Informare e formare i lavoratori sugli strumenti AI utilizzati, sulle logiche di funzionamento e sulle garanzie di controllo umano.

L'integrazione delle valutazioni: la matrice di conformità

L'approccio integrato suggerito dalla dottrina e dalle linee guida europee consiste nella costruzione di una 'matrice di conformità', che incrocia i requisiti di ciascun regime normativo con le funzioni aziendali coinvolte. Tale matrice consente di identificare le aree di sovrapposizione (ad esempio tra DPIA e risk management AI) e di ottimizzare gli sforzi di compliance. Un esempio pratico: la valutazione di trasparenza richiesta dall'art. 13 GDPR può essere soddisfatta in parte dalla documentazione tecnica dell'AI Act, mentre il monitoraggio post-market può alimentare la verifica di sicurezza ex art. 81/08.

Governance e responsabilità: chi decide cosa?

Appare evidente che vi è una parcellizzazione di responsabilità che oggi devono essere coordinate. In particolare: il General Counsel garantisce la coerenza legale e la gestione dei rischi regolatori; il DPO assicura la conformità privacy; l'HR Director supervisiona l'impatto sui lavoratori; il Chief Information Security Officer cura gli aspetti di sicurezza e resilienza; l'Organismo di Vigilanza 231 verifica i profili di responsabilità e la coerenza dei Modelli; l'Audit ha le responsabilità di verifica del rispetto dei vari modelli di compliance; e il Responsabile del Servizio di Prevenzione e Protezione valuta con l'RLS gli effetti sulla salute e sicurezza.

Output della valutazione: il fascicolo integrato AI–HR

Al termine del processo, il datore di lavoro dovrebbe poter produrre un documento unico, denominato 'Fascicolo integrato AI–HR', che raccolga tutti gli elementi di conformità: classificazione del rischio, DPIA, accordi sindacali, aggiornamento DVR, verbali di formazione e audit periodici. Questo fascicolo rappresenta la prova documentale dell'approccio sistemico dell'impresa e può essere utilizzato in sede ispettiva, giudiziale o di certificazione.

Speciali Il Punto

Il governo dell'intelligenza artificiale in azienda

di Area Innovazione e AI – StanchiStudioLegale & Partners
N. 40 - 23 ottobre 2025

Non solo compliance ma una dimensione strategica di governance per la gestione dell'intelligenza artificiale in azienda

Appare evidente che il governo dell'intelligenza artificiale in azienda non è soltanto una questione di compliance, ma una dimensione strategica della governance. L'introduzione dell'IA modifica la struttura decisionale, ridefinisce i ruoli professionali e richiede competenze trasversali capaci di coniugare diritto, tecnologia e gestione del rischio. In questa prospettiva, il futuro delle imprese sarà prevedibilmente determinato non solo dall'adozione delle tecnologie, ma dalla qualità del loro governo etico e giuridico. Non ultimo richiede gli opportuni poteri organizzativi e formali (procure ordinarie) per le eventuali attuazioni di scelte regolamentari o ostative che i processi di conformità o di verifica, dovessero imporre.

Dalla funzione legale al governo dell'innovazione

Come rileva certa attuale letteratura[1], il ruolo del General Counsel assume un significato inedito: da garante della legittimità formale diventa (o meglio pare destinato a diventare) architetto della governance dell'innovazione. In un contesto normativo frammentato e in evoluzione, è il legale d'impresa unitamente al Direttore HR che coordina le intersezioni tra AI Act, GDPR, HR, Statuto, Data Act, 231 e 81/08, assicurando che la tecnologia operi nel rispetto dei principi di proporzionalità, trasparenza e responsabilità, divenendo proattivi produttori di valore piuttosto che meri Garanti della conformità legale. La funzione legale diventa il punto di convergenza tra rischio regolatorio, etica e reputazione, agendo come vero e proprio Chief Integrity Officer. Tale centralità non esclude ma valorizza il ruolo del Chief AI Officer (CAIO), figura emergente nel panorama internazionale. Mentre il CAIO garantisce la competenza tecnica e la qualità dei modelli, il General Counsel rappresenta l'anello di collegamento con la cultura del diritto e con la responsabilità d'impresa, ed il Direttore HR rappresenta la declinazione nella struttura aziendale dei valori, anche organizzativi. Nelle realtà più complesse, le funzioni coesistono in un equilibrio dinamico; nelle PMI o nei settori tradizionali, è il General Counsel a incorporare la funzione AI governance, con il supporto di DPO, CIO e HR. In quelle complesse sono ipotizzabili strutture più articolate.

Modelli di governance ibrida: il Comitato AI

Le best practice europee (tra gli altri, BusinessEurope, DIGITALEUROPE, Anitec-Assinform) suggeriscono la creazione di un 'Comitato AI' interno alle imprese, composto da rappresentanti legali, tecnici, HR e Audit, con il compito di validare I progetti di intelligenza artificiale prima della loro adozione. L'organo ha funzioni deliberative su temi di alto impatto (alto rischio, valutazioni etiche, incidenti AI). La sua istituzione permette di dimostrare la due diligence dell'impresa e di tradurre in pratica I principi di accountability e risk management.
Il Comitato AI può anche fungere da interfaccia verso l'esterno, partecipando ai programmi di certificazione e agli hub di innovazione europei previsti dalla strategia Apply AI della Commissione (ottobre 2025). In questo

modo, la governance interna si allinea ai meccanismi di sostegno pubblico e ai modelli di innovazione responsabile promossi a livello UE.

Valutazione "senza sconti" per l'impresa (criticità e costi)

Inutile dire che almeno in una valutazione prospettica l'elefante in cristalleria c'è e probabilmente è facile che qualche danno lo produca.
AI Act

- **Sovrapposizioni** con GDPR/DPIA e Decreto Trasparenza ? rischio di compliance "a silos" e duplicazioni (FRIA vs DPIA; logging AI vs registro trattamenti).
- **Black-box dei fornitori:** requisiti high-risk scaricano su chi usa lo strumento oneri di controllo senza sempre avere trasparenza tecnica sufficiente (documentazione/metriche).
- **Temporizzazioni** e incertezza interpretativa** (linee guida in progress; ruolo dell'AI Office).
- Quanto all'attuazione italiana (L. 132/2025)
- **Legge-quadro** con **ampie deleghe:** molte scelte rinviate, per cui gli investimenti rischiano stop&go finché non arriveranno i decreti.
- **Nuovi adempimenti** (es. informazioni verso utenti/dipendenti/clienti, osservatorio, possibili ulteriori obblighi di AI literacy) con costi organizzativi immediate e ritorni incerti.

Data Act

- **Dati "misti"** (personali/non personali) in flussi IoT ? frizione continua con GDPR (minimizzazione, base giuridica, diritti interessati); rischio lock-in rovesciato (switching cloud obbligato, ma complesso).

Il tutto senza trascurare le già note complessità di GDPR, 231 e Statuto dei lavoratori. Moltissima carne al fuoco e cambiamenti di logiche organizzative (e di strumenti organizzativi) dettati dalla esponenzialità del cambiamento tecnologico. Non si tratta di istituire l'apparato, ma di governarlo costantemente rispetto ad una tecnologia che evolve esponenzialmente.
L'adattabilità darwiniana legata per ora alla sopravvivenza generazionale entra in una nuova dimensione esponenziale, che ha molti interrogativi e nessuna risposta. Forse anche l'apparato normativo va concepito come adattabile (in semplificazione esponenziale) con un monitoraggio che però è esperienza del tutto sconosciuta alle Istituzioni, lineari per necessità di sopravvivenza.

Prospettive future: la complessità come valore

Allora, per chiudere con una nota di (cupo) ottimismo forse possiamo ispirarci al Pensiero di chi, come il citato Sean West in 'Unruly', osserva che la complessità normativa non deve essere percepita come un ostacolo, ma come una condizione strutturale dei sistemi moderni. In questo contesto ambientale, l'intelligenza artificiale può diventare (non solo la fonte del problema ma) anche lo strumento per governare questa complessità, automatizzando controlli, analisi di rischio e processi decisionali interni. In poche parole gestendo la razionalità limitata del future (non per niente l'attualità e la Sovereign AI[2]) L'impresa che riesce a utilizzare l'IA per migliorare la propria capacità di compliance trasforma un obbligo in vantaggio competitivo.
In prospettiva, la convergenza tra diritto, etica e tecnologia pare destinate a delineare un nuovo modello organizzativo (globale?): non più centrato sulla semplice conformità, ma su una governance predittiva, capace di anticipare i rischi e di generare fiducia, producendo valore.

La sfida per le imprese italiane ed europee sarà quella, against all odds, di integrare la tradizione giuridica con la rapidità dell'innovazione tecnologica, costruendo un modello sostenibile di intelligenza artificiale umanocentrica, aggiungeremmo "di successo".
La sfida immediata è quella però di "mettere a terra" i) schemi organizzativi che consentano di applicare l'apparato e ii) sistemi gestionali che consentano di governarlo, producendo in tempi rapidi valore per l'azienda, le persone che vi lavorano e, in definitiva, la nostra società (per adesso ancora) civile.

[1] Cfr. Sean West, Unruly, https://www.amazon.com/Unruly-Fighting-Politics-Upend-Business/dp/1394318456

[2] Cfr. What is Sovereig AI?, https://www.oracle.com/it/artificial-intelligence/what-is-sovereign-ai

Guida al Lavoro

Settimanale di documentazione del lavoro
ISSN 1590-007X

GRUPPO 24 ORE

Proprietario ed editore
Il Sole 24 ORE S.p.A.

Presidente
MARIA CARMELA COLAIACOVO

Amministratore Delegato
FEDERICO SILVESTRI

Direttore Responsabile Roberto Esposito
Redazione Angela Grassi (02/3022.3315); Margherita Mangioni (02/3022.3695); Antonio Pesaresi (02/3022.4540)
Periodico settimanale Registrazione Tribunale di Milano n. 468 del 7 agosto 1997.
Sede legale e Direzione Viale Sarca, 223 - 20126 Milano.