



Decreto Legislativo 231/2001

Geopolitica dell' IA e l'impatto sul MOG

Ing. M. Cristina Zamparini

Ordine degli Ingegneri della Provincia di Roma

Roma, 4 marzo 2026

**Con la collaborazione di IA*



Agenda

- **La nuova frontiera del potere globale**
- **Quadro normativo**
- **L' IA e l'impatto sul D.Lgs. 231/2001**
- **L' IA e l'impatto sul Modello
Organizzativo e Gestionale (in/ extra-UE)**

La Nuova Frontiera del Potere Globale

- **Panoramica generale degli equilibri di potere**
 - **USA, Cina, Medio Oriente, Africa, Europa, Italia**
- **Frammentazione del mercato**
- **Colonialismo dei dati**
- **Infrastrutture: alcune criticità**

Strategie, Sfide e Opportunità

- L'Intelligenza Artificiale (IA) ha trasceso il suo ruolo di semplice innovazione tecnologica, affermandosi come una **leva geopolitica cruciale**.
- La **corsa al primato** in questo settore si traduce in una **competizione** che non definisce solo la supremazia tecnologica, ma **plasma** anche il **futuro economico, sociale e politico** del mondo: sta **ridisegnando gli equilibri di potere** tra grandi attori globali come gli Stati Uniti, la Cina e l'Unione Europea.
- Attori di una **rivoluzione** che influenzano lo sviluppo e l'applicazione etica dell'IA con **visioni** che rappresentano non solo **approcci** diversi allo sviluppo tecnologico, ma **filosofie** politiche e culturali profondamente differenti sulla relazione tra Stato, mercato e società che **definiranno l'architettura tecnologica globale** dei prossimi decenni



USA vs Cina: Strategie Contrapposte

Stati Uniti: Innovazione Privata

Il modello di Washington, basato sull'**iniziativa privata** e sull'innovazione aperta, favorisce uno sviluppo rapido e competitivo.

L'approccio degli Stati Uniti è caratterizzato dalla **leadership** delle loro Big a cui demandando la guida dell'innovazione e la supremazia nell'IA

Cina: Controllo Statale e industriale

Il modello di Pechino, basato sul **controllo statale** e la pianificazione centralizzata delle risorse tecnologiche e sull'integrazione l'IA in tutti i settori, favorisce il controllo sociale per rafforzare la sua potenza industriale.

L'approccio della Cina è caratterizzato da una stretta **collaborazione tra stato e industria**, finalizzata a raggiungere la leadership globale attraverso piani strategici a lungo termine.



Due Superpotenze, Due Visioni per l'AI

us Visione Americana

- Leadership del settore privato (Big Tech: Google, Microsoft, NVIDIA)
- Investimenti guidati dal mercato e dalla competizione
- Focus su innovazione aperta e ricerca accademica
- Controllo delle esportazioni per protezione strategica
- Enfasi su proprietà intellettuale e brevetti

cn Visione Cinese

- Direzione governativa attraverso piani quinquennali
- Investimenti statali massicci in infrastrutture AI
- Integrazione con obiettivi di sicurezza nazionale
- Controllo rigoroso dei dati e della privacy
- Aspirazione alla leadership tecnologica globale

L'AI e la Nuova Sovranità Digitale

Riyad-Arabia Saudita



Medio Oriente: Investimenti Strategici

Paesi come Emirati Arabi Uniti, Arabia Saudita e Qatar stanno investendo massicciamente in infrastrutture AI per diversificare dall'economia del petrolio. Il Saudi Vision 2030 ha investito \$14,9* miliardi nel settore AI con aziende tech globali.

* <https://it.investing.com/news/stock-market-news/larabia-saudita-investe-149-miliardi-nel-settore-ai-con-aziende-tech-globali-93CH-2682175>

Nairobi-Kenya



Africa: Autonomia Tecnologica

Nazioni come Nigeria, Kenya e Sudafrica sviluppano hub tecnologici locali per evitare la dipendenza da fornitori esteri. Iniziative pubblico-private mirano a creare ecosistemi AI indigeni e formare talenti locali.

Parlamento Europeo



UE: Governance Responsabile

L'Unione Europea punta a diventare il gold standard della governance AI etica.

Il framework normativo europeo bilancia innovazione tecnologica con protezione dei diritti fondamentali, creando standard che influenzano il resto del mondo.



L'Intelligenza Artificiale: uno sguardo aggiornato al 2026

88%* Adozione AI

Organizzazioni che utilizzano l'AI in almeno una funzione aziendale (McKinsey 2025)

23%* Scalabilità Enterprise

Aziende che hanno scalato l'AI a livello enterprise.
Gran parte in fase pilota

1.7x ROI Medio**

Return On Investment medio generato dalle implementazioni AI di successo

L'Intelligenza Artificiale sta attraversando una fase di crescita esponenziale, trasformando radicalmente il modo in cui le organizzazioni operano e competono nel mercato globale.

I dati più recenti rivelano una diffusione massiva ma ancora in fase di maturazione.

Un fenomeno particolarmente interessante è l'emergere degli **AI agenti intelligenti**:

sistemi che non si limitano a eseguire comandi predefiniti, ma sono **capaci di pianificare** autonomamente, **prendere decisioni in base al contesto** e **agire proattivamente** all'interno dei workflow aziendali.

Questi agenti rappresentano un **salto qualitativo dall'automazione** tradizionale all'intelligenza autonoma, aprendo nuove possibilità per la gestione aziendale ma sollevando anche **questioni complesse di governance, responsabilità e controllo** che il MOG dovrà necessariamente affrontare.

* <https://www.umbriaschool.it/quando-lai-ce-ma-non-conta-ancora-il-paradosso-utile-della-survey-mckinsey-2025/>

** <https://euroborsa.it/ai-redditivita-imprese-capgemini.aspx>



Strategia Europea ed Italiana

Unione Europea: linee guida – Regolazione Etica

- L'UE adotta un approccio più regolatorio ed etico, compiutosi nell'**AI Act**.
- Mira a **bilanciare** l'innovazione con la protezione dei diritti fondamentali e dei valori europei.
- La sfida per l'UE è quella di promuovere l'innovazione tecnologica mantenendo al contempo un quadro normativo che garantisca **fiducia, sicurezza e trasparenza nell'uso dell'IA**.

Italia: Legge 132/2025

Quadro normativo integrato:

Armonizza le regole italiane con l'AI Act europeo per un **uso responsabile** dell'intelligenza artificiale.

Principi fondamentali:

Garantisce **responsabilità umana e trasparenza**, assicurando **l'intervento umano nei processi decisionali automatizzati**.

Tutela dei diritti e etica:

Protegge la libertà politica e il dibattito democratico, ponendo **l'essere umano al centro della tecnologia e del "Diritto"**.

Implicazioni settoriali:

Disciplina l'**uso dell'IA in sanità e pubblica amministrazione** garantendo qualità, sicurezza e verificabilità.

Ing. M.Cristina Zamparini

La Frammentazione del Mercato Globale dell'AI



Normative Divergenti

Ogni regione sviluppa il proprio *framework regolamentare* per l'AI, creando un *patchwork* complesso di leggi e standard.



Controlli all'Export

Restrizioni severe su tecnologie dual-use frammentano l'ecosistema tecnologico globale e *limitano la* collaborazione internazionale.



Localizzazione Forzata

Le multinazionali devono *duplicare infrastrutture* e adattare prodotti per *conformarsi a* regolamenti nazionali diversi.

Europa: GDPR e AI Act

Il (GDPR) e AI Act impongono standard etici rigorosi.

Le aziende devono implementare principi come "privacy by design" e garantire trasparenza negli algoritmi, con sanzioni fino al 7%* del fatturato globale.

USA: Export Controls

Il Dep. Commerce ha inserito nell'Entity List decine di aziende cinesi, vietando loro l'accesso a tecnologie avanzate.(GPU NVIDIA)

Restrizioni specifiche su chip di ultima generazione limitano la capacità produttiva di concorrenti strategici.

Cina: Data Sovereignty

La legge sulla Sicurezza dei Dati e la Cybersecurity Law richiedono che i dati dei cittadini cinesi siano archiviati e gestiti localmente.

Le aziende straniere devono formare joint venture con partner locali e condividere codice sorgente per operare nel mercato.

* <https://www.cybersecurity360.it/news/ai-act-scattano-i-primi-divieti-chi-rischia-le-sanzioni-e-le-prossime-tappe/>

La Diplomazia Tecnologica Contro il Colonialismo dei Dati

- Il termine "**colonialismo dei dati**" descrive la *concentrazione di dati e capacità analitiche nelle mani di poche multinazionali e/o governi*.
- Paesi emergenti rispondono con strategie di "**diplomazia tecnologica**": *accordi bilaterali* per scambio di tecnologie, investimenti in infrastrutture locali, e creazione di *alleanze regionali* per contrastare l'*egemonia tecnologica*.
- La **sovranità tecnologica** diventa così strumento di *indipendenza politica ed economica*, permettendo ai paesi di controllare le proprie risorse informative e di sviluppare capacità strategiche autonome.



Infrastrutture Critiche: Il Cuore Pulsante della Geopolitica AI

- Ogni chip AI, ogni algoritmo di machine learning, ogni sistema di riconoscimento vocale dipende da una **infrastruttura fisica** di calcolo massivo che **richiede energia, raffreddamento e sicurezza fisica**.
- La geografia di queste infrastrutture definisce chi controlla il **potere computazionale**.
- Stati Uniti e Cina ospitano il 70%* dei data center con *capacità di calcolo AI di fascia alta. (Hyperscale)*
- L'UE cerca di colmare il gap con il programma **EuroHPC** per supercomputer dedicati alla ricerca europea.
- Il primo **sistema EuroHPC per calcolo quantistico** in Europa ed è stato installato in Italia. Si tratta di [EuroQCS-Italy](#), un computer quantistico a *neutral atoms* sviluppato da **Pasqal** e consegnato al DAMA Tecnopolo di Bologna presso il **CINECA**. si inserisce nel piano europeo per lo sviluppo di **un'infrastruttura sovrana di sistemi ibridi**, con l'obiettivo di *“rafforzare la competitività della ricerca e delle imprese”* e consolidare il **“ruolo dell'Italia come hub strategico per supercalcolo, intelligenza artificiale e tecnologie quantistiche”**. (19-02-2026)**
- Intanto, paesi come Islanda e Norvegia attraggono investimenti grazie all'energia geotermica a basso costo e al clima favorevole al raffreddamento naturale.

* <https://www.cargoson.com/it/blog/numero-di-data-center-per-paese>

** <https://www.key4biz.it/vlq-avviato-il-nuovo-computer-quantistico-europeo-video/547886/>

350+

Data Center Strategici

Installazioni critiche monitorate
globalmente per capacità di calcolo AI

200MW

Consumo Energetico Medio

Potenza elettrica necessaria per
alimentare un data center di fascia alta

\$25B

Investimenti Annuo Globali

Spesa in nuove infrastrutture
di calcolo per AI nel 2025

* Rasmus Leichter (2025). "Numero di Data Center per Paese (Novembre 2025)". Retrieved from <https://www.cargoson.com/it/blog/numero-di-data-center-per-paese>

INFRASTRUTTURE CRITICHE

IL CUORE PULSANTE DELLA GEOPOLITICA AI



Agenti AI: Abilità e allucinazioni



ChatGPT

Conversational AI &
Content Creation



DALL-E

AI Art & Image Generation



Whisper

Speech Recognition
& Transcription



Sora

AI Video Generation & Simulation



Codex

AI Code Assistance



Ada

Data Analysis & Insights



CLIP

Vision & Language
Understanding



GPT-4

Advanced Large Language Model



Robo

AI Assistance & Automation



Gamma

AI Presentation & Document Creation



Copilot

Integrated AI Assistance



Gemini

Multimodal AI & Language Understanding

Immagine generata da
un Agente AI.

Non è riuscito a
mostrare il suo vero
logo.

Alcuni sono “inventati”
ha creato
un’allucinazione

Quadro Normativo

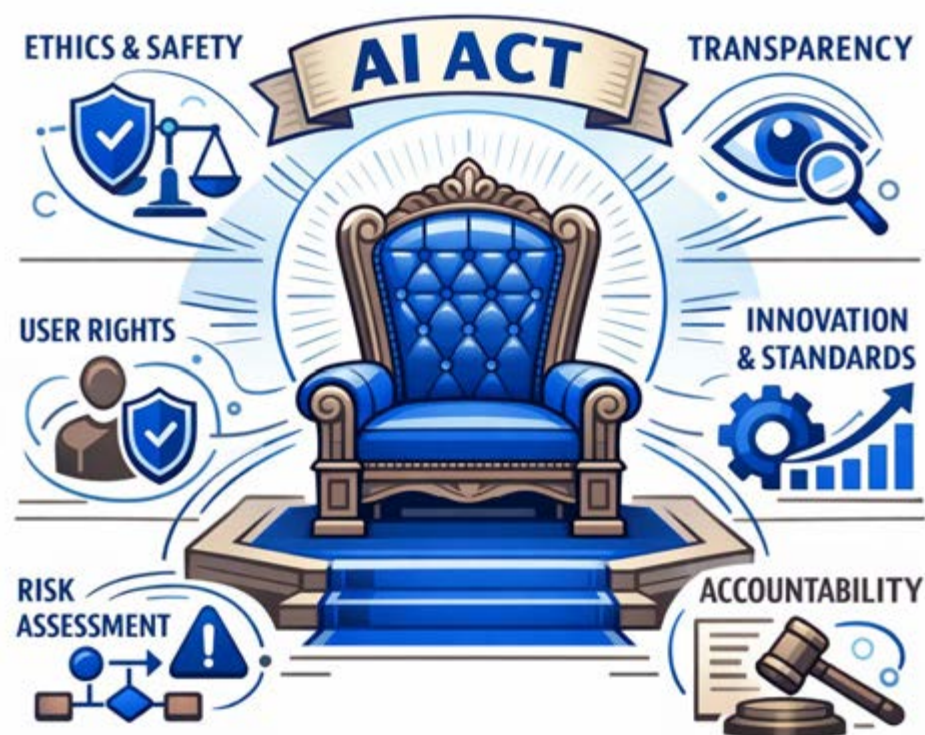
- **EUROPA**

Regolamento (UE) 2024/1689 AI-act

- **ITALIA**

Legge 132 del 23 Settembre 2025

Legge Italiana sull'Intelligenza Artificiale (132/2025)



AI-act i livelli di Rischio (1/2)

Obblighi crescenti

In base al *potenziale impatto* dell'AI sulla sicurezza, sulla salute e sui diritti fondamentali delle persone.



Livello 1 – Rischio Minimo

Riguarda la maggior parte delle *applicazioni di AI*, come *videogiochi*, *filtri antispam*, *sistemi di raccomandazione generici*.

Non sono previsti obblighi normativi aggiuntivi

Livello 2 – Rischio Limitato

Comprende sistemi che richiedono **obblighi di trasparenza**, come:

- chatbot *devono informare l'utente di interagire con una macchina*,
- sistemi che generano deepfake, *devono dichiarare la natura artificiale del contenuto*.

L'obiettivo è permettere **scelte consapevoli** all'utente.

Livello 3 – Rischio Alto

È la categoria **più regolamentata**.

Un sistema è considerato ad alto rischio se:

- è *un componente di sicurezza di prodotti soggetti a legislazione UE* (es. dispositivi medici, macchinari, automobili, aviazione), e richiede **valutazione di conformità**;
- rientra in *casi d'uso specifici elencati nell'Annex III* (es. occupazione, giustizia, infrastrutture critiche, istruzione, credito). *

Alcuni sistemi elencati nell'Allegato III possono essere esclusi dalla categoria "alto rischio" se svolgono solo compiti procedurali o preparatori senza influenzare decisioni e senza profilare persone. * *

Gli **obblighi** includono:

- qualità dei dati
- gestione del rischio
- documentazione tecnica dettagliata
- supervisione umana
- robustezza e cybersecurity

* <https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-6> e <https://euairisk.com/resources/eu-ai-act-high-risk-requirements>

** <https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-6>

Livello 4 – Rischio INACCETTABILE

Si tratta di pratiche vietate in modo assoluto, perché considerate contrarie ai valori dell'UE:

- sistemi di manipolazione (come tecniche *subliminali*),
- social scoring,
- identificazione *biometrica remota* in tempo reale in spazi pubblici (salvo eccezioni ristrette).

Queste pratiche sono escluse dal mercato europeo





Legge 132 del 23 Settembre 2025

Finalità e Principi fondamentali

Principio antropocentrico

L'essere umano rimane *responsabile ultimo* delle decisioni automatizzate o ad alto rischio in IA.

Prevenzione discriminazioni e privacy

I sistemi IA devono *prevenire discriminazioni*, distorsioni sistemiche e tutelare la *privacy degli utenti*.

Trasparenza nell'uso dell'IA

Le organizzazioni devono *informare chiaramente* quando decisioni o servizi derivano da IA.

Sicurezza e innovazione etica

La legge promuove sistemi IA sicuri, etici e conformi alle normative europee per innovazione sostenibile.

Principi e Regole Operative

Trasparenza nelle interazioni IA

Le organizzazioni devono informare gli utenti sull'uso di sistemi IA, soprattutto in ambiti sensibili come banca e sanità.

Sicurezza e monitoraggio continuo

I sistemi IA devono essere sottoposti ad *audit*, vulnerabilità controllate e protezioni come crittografia e accesso controllato.

Qualità e legalità dei dati

È obbligatorio utilizzare *dati accurati, aggiornati e acquisiti legalmente*, evitando bias e distorsioni dannose.

Divieto di text & data mining illecito

La legge proibisce l'estrazione e riproduzione di dati protetti senza autorizzazione, richiedendo valutazione rigorosa delle licenze.

Governance e Strutture di Controllo

Livello di governance nazionale

AgID *promuove* e accredita i sistemi di IA, mentre **ACN** *vigila*, ispeziona e applica sanzioni.

Governance interna alle organizzazioni

Le aziende definiscono ruoli chiave, *responsabili IA* e comitati interdisciplinari per monitorare rischi e conformità.

Integrazione di IA nei processi aziendali

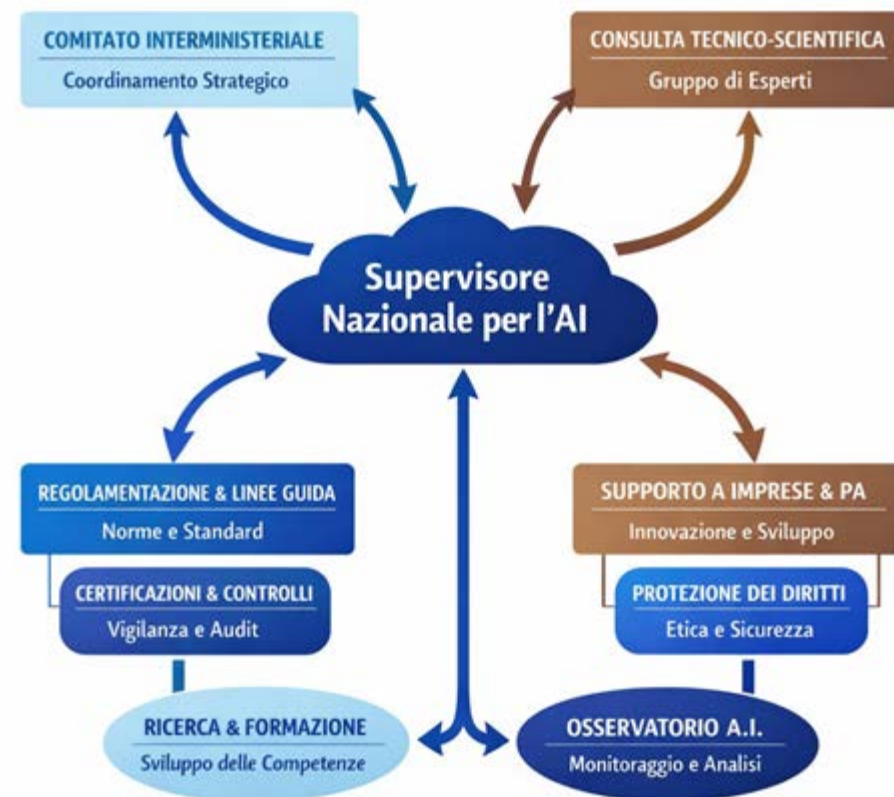
L'IA va integrata in audit, risk management e compliance *aggiornando strumenti come il Modello 231/2001*.

Prevenzione e collaborazione normativa

La governance multilivello previene violazioni e dimostra collaborazione con autorità durante accertamenti e sanzioni.

GOVERNANCE AI

Legge Italiana sull'Intelligenza Artificiale (132/2025)



Applicazioni Settoriali e Sanzioni

Settori strategici regolati

La legge 132/2025 regola *sanità, lavoro, pubblica amministrazione, giustizia e cybersicurezza* per garantire un uso responsabile dell'IA.

Supervisione umana e trasparenza

L'IA *supporta* decisioni mediche e amministrative, ma la *supervisione umana resta obbligatoria* e l'uso deve essere trasparente.

Sistema sanzionatorio severo

Sanzioni includono multe fino al 7%* del fatturato globale e nuove fattispecie penali per gli abusi di IA come deepfake e mining non autorizzato.

Incentivi per politiche aziendali

La normativa incentiva l'adozione di *politiche rigorose* e la *formazione* del personale per un uso corretto delle tecnologie intelligenti.

• <https://www.altalex.com/documents/news/2025/02/03/ai-act-vigore-divieto-sistemi-rischio-inaccettabile>

Ing. M.Cristina Zamparini

Geopolitica dell' IA e l'impatto sul MOG

SANZIONI AMMINISTRATIVE

Legge Italiana sull'Intelligenza Artificiale (132/2025)



L' IA e l'Impatto sul D.Lgs. 231/2001

- **Nuovi reati**
- **Linee guida per l'integrazione dell'IA in Azienda**

L'Intelligenza Artificiale: una rivoluzione normativa e aziendale

Legge 132/2025:

Il Primo Quadro Organico Italiano sull'IA

La Legge 132/2025 rappresenta una **pietra miliare** nel contesto normativo italiano, istituendo il primo quadro organico e completo per la disciplina dell'Intelligenza Artificiale. Questa legislazione si allinea strettamente con l'**AI Act** (Regolamento UE 2024/1689), mirando a creare un **ecosistema armonizzato** per l'IA a livello europeo. L'Italia si posiziona all'avanguardia nell'affrontare le complessità etiche e giuridiche dell'innovazione tecnologica.

Obiettivo:

Uso Etico, Trasparente e Responsabile

L'obiettivo primario della Legge 132/2025 è garantire un **utilizzo** dell'IA **etico, trasparente e responsabile**, ponendo al centro la tutela dei diritti fondamentali degli individui. Quindi le aziende dovranno implementare **sistemi di IA** che rispettino la privacy, non siano discriminatori e siano controllabili dall'uomo, promuovendo al contempo l'innovazione in un contesto di sicurezza giuridica.

Impatto Diretto sulle Imprese: Nuove Responsabilità e Rischi

L'introduzione di questa nuova normativa ha un impatto profondo sulle aziende, che si trovano ad affrontare **nuove responsabilità e rischi** legati all'implementazione e all'uso dei sistemi di IA. Questo include la necessità di rivedere i processi interni, adattare i modelli organizzativi e investire in nuove competenze per mitigare i potenziali danni e garantire la conformità.

- **Introduzione del reato di diffusione illecita di deepfake**

L'articolo **612-quater** del **Codice Penale** è stato aggiornato per includere esplicitamente il reato di diffusione illecita di deepfake.

Questo reato mira a contrastare la manipolazione digitale di immagini o video che alterano la realtà, creando contenuti falsi ma estremamente realistici, con potenziali danni alla reputazione e alla dignità delle persone.

La norma prevede sanzioni severe per coloro che creano o diffondono tali contenuti senza consenso, specialmente se a scopo di nuocere.

- **Abuso di tecniche di web scraping e data mining con IA**

L'utilizzo di tecniche avanzate di web scraping e data mining, soprattutto se potenziate da sistemi di Intelligenza Artificiale, può configurare un reato ai sensi dell'articolo **171 della Legge 633/1941**, che tutela il diritto d'autore.

Questo articolo viene interpretato in modo più ampio per coprire l'estrazione massiva e non autorizzata di dati protetti da copyright o da banche dati, quando tale attività è finalizzata a scopi commerciali o di concorrenza sleale, specialmente se compiuta da algoritmi di IA.

- **Aggravanti specifiche per reati di aggio e manipolazione del mercato**

Sono state introdotte **aggravanti** specifiche per i reati di aggio e manipolazione del mercato, qualora questi vengano commessi attraverso l'uso di sistemi di Intelligenza Artificiale.

Questo riflette la *crescente consapevolezza del potenziale impatto dell'IA sulle dinamiche finanziarie*, dove algoritmi sofisticati possono essere utilizzati per influenzare i prezzi, diffondere false informazioni o compiere operazioni fraudolente sui mercati.

- **Ampliamento dei reati presupposto**

Le aziende dovranno aggiornare i propri Modelli di Organizzazione, Gestione e Controllo (MOGC) *per includere presidi atti a prevenire la commissione di tali reati anche attraverso l'uso, intenzionale o colposo, di sistemi di IA*.

La mancata previsione e prevenzione di questi rischi potrebbe esporre l'ente a sanzioni significative poichè verrebbe a perdere le connotazioni tipiche di un MOG esimente.



Rispetto dei Diritti Fondamentali, Trasparenza e Proporzionalità

L'adozione di sistemi di Intelligenza Artificiale nelle aziende deve essere guidata da **principi cardine**.

È **imperativo** garantire il pieno **rispetto dei diritti fondamentali**, assicurando che l'IA non introduca discriminazioni, violazioni della privacy o altre lesioni alla dignità umana.

La **trasparenza** richiede che le *decisioni prese dagli algoritmi siano comprensibili e spiegabili*, mentre la **proporzionalità** impone che l'*uso dell'IA sia adeguato e necessario rispetto agli obiettivi perseguiti*, evitando un impatto eccessivo sugli individui.



Sorveglianza e Intervento Umano Obbligatori

Anche nei sistemi di IA più avanzati, la **sorveglianza e l'intervento umano rimangono un elemento cruciale**.

La Legge 132/2025 stabilisce l'**obbligo** di *garantire un controllo significativo da parte dell'uomo* (human-in-the-loop) sui sistemi di IA, specialmente quelli *ad alto rischio*.

Questo assicura che gli operatori possano monitorare, interpretare e, se necessario, intervenire per correggere le decisioni dell'IA, prevenendo danni e *garantendo la responsabilità ultima*.



Prevenzione di Interferenze illecite

Un aspetto delicato riguarda la **prevenzione** di interferenze illecite nella vita istituzionale e politica.

I sistemi di IA **non** devono essere **utilizzati** per manipolare l'opinione pubblica, influenzare processi elettorali o destabilizzare le istituzioni democratiche.

Le aziende devono adottare **misure rigorose** per *evitare che i propri strumenti* di IA vengano impiegati per scopi che minano i principi democratici e la libertà di espressione.



Cybersecurity come Precondizione Essenziale

La cybersecurity è una **precondizione fondamentale** per l'affidabilità e la sicurezza di qualsiasi sistema di IA.

La **protezione** dei dati e delle infrastrutture su cui l'IA si basa deve essere garantita lungo tutto il ciclo di vita del sistema, dalla progettazione all'utilizzo e alla dismissione.

Ciò include la *difesa contro attacchi informatici*, la *protezione da vulnerabilità* e la *resilienza operativa*, essenziali per prevenire usi malevoli o malfunzionamenti che potrebbero avere conseguenze gravi.

Percorso per l'integrazione Responsabile dell'Intelligenza Artificiale conforme al D.Lgs. 231/2001

il percorso strategico per le imprese



Ogni fase, dall'adozione dell'AI all'aggiornamento del modello 231 e alla formazione, **è cruciale** per garantire un *utilizzo etico e sicuro dell'IA stessa*, minimizzando i rischi legali e reputazionali

L' IA e l'impatto sul Modello Organizzativo e Gestionale

- **Impatti Operativi e Strategici**
- **Mercati extra-UE :**
 - **Esportazione e**
 - **Extraterritorialità dell'AI Act europeo**



Come l'AI influisce sul MOG

(1/3)

L'integrazione dell'Intelligenza **A**rtificiale nei **M**odelli **O**rganizzativi sta producendo cambiamenti tangibili e misurabili in diverse aree aziendali.

Ecco i principali impatti osservati nelle organizzazioni all'avanguardia.

Impatto Operativo

- Riduzione consistente dei tempi di processo
- Analisi di dati complessi in secondi invece di settimane
- Monitoraggio 24/7 senza *fatigue* umana
- Scalabilità istantanea delle capacità analitiche

Impatto Strategico

- Identificazione di opportunità di mercato nascoste
- Simulazione di scenari futuri con accuratezza superiore
- Supporto decisionale basato su evidenze
- Aggiornamento continuo delle strategie



Automazione Intelligente Compliance

Sistemi AI per **monitoraggio continuo** della compliance normativa e **gestione proattiva dei rischi**, riducendo significativamente gli errori umani e aumentando di conseguenza l'efficienza del controllo interno



Thought Partner Strategico

AI come **partner di pensiero nella definizione strategica**, capace di analizzare migliaia di scenari simultaneamente, identificare *pattern nascosti* e suggerire opzioni strategiche basate su dati (McKinsey 2025)



Riprogettazione Workflow

Trasformazione fondamentale dei **processi operativi** per integrare l'AI in modo nativo, migliora efficienza e capacità di innovazione specialmente nelle delle aziende high performer.

* <https://www.umbriaschool.it/quando-lai-ce-ma-non-conta-ancora-il-paradosso-utile-della-survey-mckinsey-2025/>



Come l'AI influisce sul MOG

(3/3)

Questa evoluzione non solo tecnologica richiede una **ridefinizione** dei processi decisionali, della governance e **della cultura aziendale** per abbracciare pienamente le opportunità offerte dall'AI **senza compromettere** i *principi di controllo e responsabilità* *trasparenza e conformità* che sono il **cuore del modello organizzativo**.

Comitato di Governance AI

Struttura cross-funzionale di alto livello che definisce strategia, policy e principi etici per l'uso dell'AI nell'organizzazione

Team di Implementazione

Unità dedicate che coordinano l'integrazione dell'AI nei processi, gestiscono vendor esterni e assicurano qualità tecnica

Funzione di Controllo

Role specifico per monitoraggio continuo, testing di bias, validazione risultati e verifica compliance degli algoritmi AI



Aziende Italiane: MOG + AI + Extra-UE = Esposizione ai Rischi 231

Quadro Generale:

Per le aziende italiane che *esportano servizi AI in mercati extra-UE*, i rischi non si limitano più ai tradizionali aspetti commerciali.

Dal **24-01-2026** con l'entrata in vigore del **D.Lgs. 211/2025**

«Attuazione della direttiva 2024/1226/UE del Parlamento europeo e del Consiglio, del 24 aprile 2024, relativa alla definizione dei reati e delle sanzioni per la violazione delle misure restrittive dell'Unione e che modifica la direttiva (UE) 2018/1673».

le violazioni delle misure restrittive europee e dell'export control sono diventate **reati presupposto 231**, con effetto diretto sulle aziende che operano fuori dall'UE, inclusi servizi immateriali come l'AI. [\[alpimelissa.com\]](https://www.alpimelissa.com) <https://www.alpimelissa.com/sanzioni/sanzioni-ue-231/>

L'aggiunta del nuovo **art. 25-octies.2** *amplia enormemente il perimetro del rischio* per le imprese dell'AI che esportano software, algoritmi, modelli o servizi digitali in Paesi soggetti a restrizioni. [\[laborproject.it\]](https://laborproject.it)

<https://laborproject.it/2026/01/20/violazione-delle-misure-restrittive-ue-e-responsabilita-231-il-passaggio-dal-sistema-per-quote-alle-sanzioni-sul-fatturato/>



Aziende Italiane: MOG + AI + Extra-UE = Esposizione ai Rischi 231 Principali Problematiche (1/3)

1. Rischi legati alle sanzioni UE ed export control

Le imprese che forniscono servizi AI verso mercati extra-UE *possono incorrere in reati 231* se:

- esportano tecnologia verso Paesi soggetti a restrizioni UE (es. Russia, Iran, Siria)
- forniscono software o modelli AI classificabili come **dual use**
- vendono servizi AI a soggetti presenti nelle lista «sanctioned entities»

Secondo il D.Lgs. **211/2025** l'azienda può essere *ritenuta responsabile anche per condotte colpose legate a errori organizzativi o mancate verifiche*. [\[alpimelissa.com\]](https://www.alpimelissa.com)

<https://www.alpimelissa.com/sanzioni/sanzioni-ue-231/>

Le sanzioni possono arrivare fino al **5%** del fatturato globale, superando di *gran lunga il sistema tradizionale “a quote” previsto dal 231*. [\[laborproject.it\]](https://laborproject.it)

<https://laborproject.it/2026/01/20/violazione-delle-misure-restrittive-ue-e-responsabilita-231-il-passaggio-dal-sistema-per-quote-alle-sanzioni-sul-fatturato/>

Aziende Italiane: MOG + AI + Extra-UE = Esposizione ai Rischi 231

Principali Problematiche (2/3)

2. Extraterritorialità dell'AI Act europeo

Anche per i servizi AI erogati in Paesi extra-UE, *l'AI Act si applica quando:*

- il servizio AI produce output utilizzati all'interno dell'UE
- il modello è accessibile da utenti europei
- un cliente extra-UE utilizza il servizio verso target europei

Ciò comporta che un'azienda italiana che esporta AI deve rispettare gli obblighi dell'AI Act anche quando opera in Paesi terzi.

<https://intelligens.africa/2025/07/04/extraterritorial-application-of-the-eu-ai-act-what-non-eu-companies-should-know/>

In particolare per i sistemi ad *alto rischio* (es. riconoscimento biometrico, scoring algoritmico, modelli che incidono su diritti fondamentali), vi sono obblighi documentali, audit, tracciabilità e qualità dei dataset.

<https://cms.law/en/int/publication/guide-to-the-eu-ai-act-for-businesses-outside-the-eu>

Aziende Italiane: MOG + AI + Extra-UE = Esposizione ai Rischi 231 (3/3)

Principali Problematiche

3. Rischi di reati 231 commessi mezzo AI

La normativa italiana del 2025–2026 ha introdotto *nuove fattispecie di reato* che possono essere integrate tramite strumenti di IA, ad es.:

- *manipolazione* del mercato o *aggiotaggio* tramite algoritmi di trading
- violazione del *diritto d'autore* tramite modelli generativi
- diffusione di deepfake utilizzabili per frodi o reati informatici
- frode informatica o trattamento illecito di dati tramite sistemi AI

La Legge 132/2025 *riconosce che l'IA* può essere uno strumento di commissione del reato, aumentando l'esposizione 231.

<https://www.gsep.it/2026/01/10/intelligenza-artificiale-e-modello-231/>

4. Rischi organizzativi per il Modello 231

Le aziende che usano o producono AI possono incorrere in:

- *carenze nella mappatura* dei rischi legati ai nuovi processi automatizzati
- assenza di protocolli adeguati per AI ad alto rischio
- *mancata formazione del personale nell'uso corretto dei sistemi AI*
- flussi informativi insufficienti verso l'Organismo di Vigilanza (OdV)

Il MOG deve essere aggiornato per includere rischi, controlli e governance dell'AI.

<https://paradigma.it/2026/02/19/decreto-231-sanzioni-ue-aggiornamento-mog-231/>



Aziende Italiane: MOG + AI + Extra-UE = Esposizione ai Rischi 231 (1/2)

Come affrontare le Problematiche

1. Aggiornamento del Modello 231 (MOG)

Le imprese come da aggiornamenti normativi implementano:

- revisione del risk assessment 231 includendo i rischi AI, export e sanzioni
- protocolli specifici per export control e due diligence sulle controparti
- procedure di audit di algoritmi, dataset e processi decisionali automatizzati
- integrazione dell'AI all'interno dei processi esistenti di compliance

<https://paradigma.it/2026/02/19/decreto-231-sanzioni-ue-aggiornamento-mog-231/>

2. Sanzioni Due Diligence e verifiche sulle controparti

Per evitare violazioni 231 e UE le attività considerate essenziali dopo il D.Lgs 211/2025 sono:

- utilizzo di piattaforme come EU Sanctions Map
- implementazione di strumenti di screening automatizzato
- verifica di destinazione, uso finale, partner e filiera

<https://www.altalex.com/documents/news/2026/02/15/sanzioni-ue-svolta-231-nuovo-d-lgs-211-2025-cambia-regole-per-imprese>



Aziende Italiane: MOG + AI + Extra-UE = Esposizione ai Rischi 231 (2/2)

Come affrontare le Problematiche

3. Conformità all'AI Act per servizi destinati a Paesi extra-UE

Le aziende, secondo la *Guida Operativa* dovrebbero:

- determinare la categoria di rischio dei sistemi AI
- documentare dataset, controlli, audit e sicurezza del modello
- predisporre contratti con clausole che limitino l'uso dell'AI nell'UE se non conforme
- garantire trasparenza e supervisione umana

<https://natlawreview.com/article/extraterritorial-scope-eu-ai-act/>

4. Formazione del personale e nuova governance interna

Le imprese, secondo Studi mostrano la necessità crescente di investire in:

- programmi di AI literacy
- formazione su rischi legali e operativi dell'AI
- definizione di ruoli interni per la governance della tecnologia (AI compliance officer)

<https://www.augustasrisk.com/blog/intelligenza-artificiale-e-modello-231-come-cambia-la-governance-aziendale-con-lai-act/>

5. Audit tecnologici periodici e monitoraggio continuo

Pratiche di governance raccomandate da AI Act e dal nuovo assetto 231:

- audit periodici sui modelli
- test di robustezza, accuratezza e bias
- revisione continua del ciclo di vita dell'AI

<https://www.agendadigitale.eu/industry-4-0/legge-ai-e-compliance-231-come-cambia-la-responsabilita-dimpresa/>

Conclusione: Il MOG di domani

L'evoluzione del **MOG** nell'era **AI** non è un'opzione ma una **necessità strategica** per le organizzazioni che vogliono rimanere **competitive nel mercato globale del futuro**.

La **sfida** principale consiste nel **bilanciare** efficacemente il *controllo organizzativo*, *l'innovazione tecnologica* e *l'agilità operativa* in contesti aziendali complessi e dinamici

Questo richiede una **visione strategica chiara**, **leadership determinata**, **investimenti nelle competenze** e una **cultura aziendale aperta al cambiamento** il tutto è fondamentale anche per mantenere la *fiducia degli stakeholder* e *assicurare che i benefici dell'AI superino i rischi*.



Fondamenta Robuste

Mantenere principi solidi di **governance e controllo** come base



Evoluzione Continua

Adattare **processi e responsabilità** alle nuove tecnologie AI



Competitività

Trasformare il MOG in **vantaggio strategico**



mcristina.zamparini@protonmail.com

Ing. M. Cristina Zamparini