

SEMINARIO

A.I. e l'impatto sui modelli Organizzativi Gestionali (MOG)



Ing. Roberto Francini

*Presidente Commissione 231 e modelli organizzativi
Ordine degli Ingegneri della Provincia di Roma*



Obiettivo della presentazione:

« IN UNA BELLA GALOPPATA CERCHERO' DI SOLLECITARE ALCUNE RIFLESSIONI CON **FLASHES ETICO /TECNICI** SULLA INTRODUZIONE DELLA **AI** NELLA VITA E SVILUPPO DELLE IMPRESE E SOCIETA' »

- Effetti che l'innovazione introdotta dall'Intelligenza Artificiale (AI) negli Enti e nelle Imprese può avere sulla redazione del **Modello Operativo Gestionale 231/01**
- Principali possibili **vantaggi** di software AI in ambito lavorativo e sicurezza.
- Principali possibili **nuovi rischi** e minacce nel contesto etico
- La nuova normativa in **tema di responsabilità** da colpa di organizzazione dell'ente che abbia affidato la gestione del proprio MOG ad un software AI
- La struttura di una **nuova compliance**

SECTION

2 cenni di richiamo sul DLGS 231
E Modello Organizzativo Gestionale –MOG-

01

Obiettivo del DLGS 231/01



Il D.lgs. n. 231/2001 introdusse una grande novità per il diritto d'impresa, ponendo a carico delle società una responsabilità amministrativa/penale per

1. una serie di reati commessi da propri amministratori, dirigenti, dipendenti o terzi mandatari, definiti apicali
2. qualora siano stati realizzati nell'interesse o a vantaggio dell'impresa e
3. siano stati resi possibili da carenze della struttura organizzativa dell'impresa stessa.

Le società possono sottrarsi a responsabilità – e quindi alle relative sanzioni – qualora abbiano adottato, prima della commissione del fatto-reato, un idoneo Modello Organizzativo e Gestionale, predisposto ai sensi del Decreto 231 (in breve MOG231) , **dimostrando di aver fatto il possibile per evitare il reato.**



Responsabilità dell'Ente

Come può l'ente/azienda dimostrare di non essere responsabile per un reato commesso da un suo dipendente apicale ?

- L'ente potrebbe essere **esente da responsabilità** se prova, di aver adottato un modello ("MOGC") adeguato, o se la persona che ha commesso il reato è riuscita a commetterlo eludendo fraudolentemente il modello.
- **Le sanzioni potrebbero essere evitate**, in altri, notevolmente ridotte se l'ente si è adoperata per recuperare rapidamente le carenze ad essa contestate con le conseguenze provocate dall'illecito/reato .
- Appare evidente che nei reati 231 la dimostrazione di aver adottato le **misure logiche e organizzative idonee è fondamentale**.

Che succede se il MOGC è stato redatto e aggiornato da una AI generativa o agentic AI ?

SECTION

AL CUORE DEL PROBLEMA

02



Cosa sta entrando nelle nostre vite ?

L' introduzione della Intelligenza Artificiale GENERATIVA

- ✓ L'Industry 4.0 ha abilitato l'automazione e la connettività
- ✓ L'Industry 5.0 ha portato l'attenzione su
- ✓ persone, resilienza e sostenibilità
- ✓ Le Smart Factory integrano sistemi, dati e persone in modo dinamico
- ✓ Il principio di Human-in-the-loop garantisce equilibrio tra uomo e macchina.

1950's	 Artificial intelligence (AI) <i>Human intelligence exhibited by machines</i>
1980's	 Machine learning <i>AI systems that learn from historical data</i>
2010's	 Deep learning <i>Machine learning models that mimic human brain function</i>
2020's	 Generative AI (Gen AI) <i>Deep learning models (foundation models) that create original content</i>

Progettare soluzioni che mantengano l'essere umano al centro,
“ human-in-the-loop ” garantisce il rispetto dei **valori umani e sociali**.

**Oggi una nuova tecnologia sta ridefinendo il modo in cui
fabbriche e sistemi industriali; apprendono, reagiscono e
prendono decisioni in modo autonomo:**

l'Intelligenza Artificiale Generativa e Agentic AI



GEN AI + Retrieval Augmented Generation

GenAI è un tipo di intelligenza artificiale che utilizza modelli di apprendimento automatico per creare contenuti nuovi, come testi, immagini, audio, video e codice. La GenAI impara da grandi set di dati per generare output che riflettono schemi e caratteristiche apprese, ed è in grado di produrre contenuti originali su richiesta, basati su prompt ricevuti

La **Retrieval Augmented Generation (RAG)**, una tecnica che consente di estendere il foundation model di una Gen AI all'utilizzo di fonti pertinenti al di fuori dei dati di addestramento. La **Retrieval-Augmented Generation (RAG)** è quindi un sistema che aiuta a dare risposte migliori e più pertinenti.

1. Retrieval (Ricerca): L'IA cerca informazioni rilevanti in un database o una fonte di conoscenza **esterna** in casi simili .



2. Generation (Generazione): Utilizza i dati trovati durante la ricerca per generare risposte più accurate ed attuarle .



Risposta tradizionale (AI senza RAG): L'IA usa solo ciò che sa dal suo addestramento.



Risposta con RAG: L'IA cerca informazioni aggiornate in rete per dare risposte migliori.

GenAI in fabbrica oggi

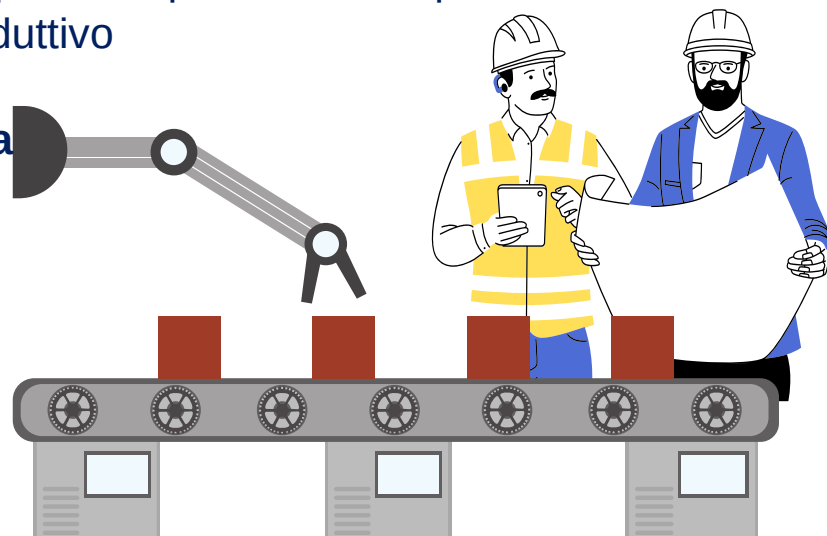
Esempio di evidenti vantaggi

Gli operatori di linea si trovano spesso a dover:

- Consultare manuali tecnici complessi durante l'attività operativa, rallentando l'intervento.
- Gestire **anomalie** senza istruzioni immediate e contestuali
- Lavorare in ambienti dove un errore operativo può avere impatti sulla **sicurezza personale** e sul processo produttivo
- Dipendere da **documentazione dispersa**



Tempi di fermo più lunghi
Conoscenza tecnica poco accessibile
Riduzione della sicurezza operativa



Assistente all'operatore di linea

GenAI



- ✓ Risponde in tempo reale a domande su manuali, procedure, parametri e anomalie.
- ✓ Comprende il linguaggio naturale, anche tecnico
- ✓ Accede alla documentazione aziendale (PDF, database, note operative).
- ✓ Si integra con la linea per fornire risposte contestuali.
- ✓ Aumenta la sicurezza riducendo gli errori legati a interpretazioni sbagliate.
- ✓ Supporta l'autonomia e la formazione continua dell'operatore.



Sfide nell'uso dell'AI in campo industriale

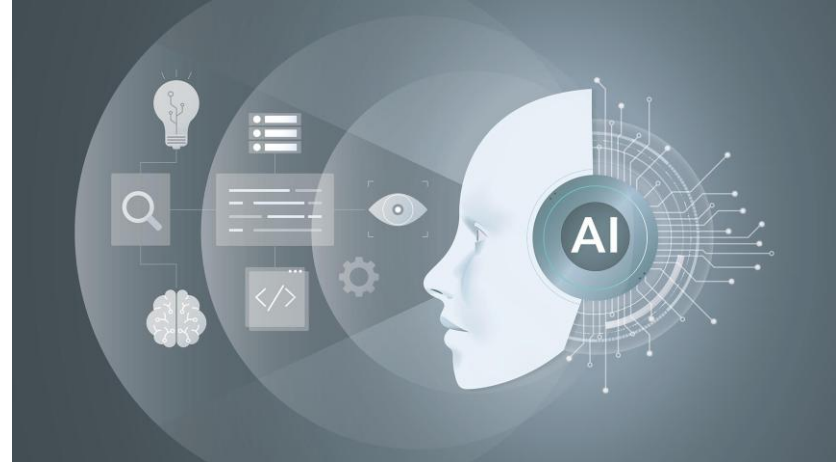
Il miglioramento delle prestazioni è in linea con le tutele della privacy e dei lavoratori , della situazione, a volte particolare, che esiste in società ?

E' sicuramente in linea con quanto assorbito dalle reti neurali a cui la dedicata AI è collegata , ma vi sono perplessità:

- Limiti tecnici nel **caricare documentazione complessa** (tipica del settore industriale);
- In ambito HSE, manutenzione o controllo qualità, un errore della GenAI può causare **danni fisici, economici o ambientali!**
- L'addestramento o l'uso della GenAI su dati aziendali solleva domande su **riservatezza, proprietà intellettuale e consenso;**
- Attenzione al controllo del **bias nei dati** (es. manutenzione trascurata in certi impianti o operatori meno esperti penalizzati).

AI gen **versus** Agent AI

Una più avanzata AI sta entrando – è entrata- nel nostro vivere quotidiano



La generazione di intelligenza artificiale è un'intelligenza artificiale generativa (**GenAI**), una tecnologia **reattiva** che crea contenuti come testo o risposte a partire da un prompt di un operatore.

Gen AI è uno strumento che crea nuovi contenuti in risposta a un prompt. Può essere un componente di un sistema agente più grande, ma non agisce da solo per svolgere un compito o un azione.

AI agentic diventa un «**agente proattivo** » dell'utente e/o del sistema e si occupa di risolvere il compito che gli è stato assegnato inizialmente .

Ponendo l'accento sul comportamento orientato agli obiettivi, l'intelligenza artificiale agentic può portare a termine i compiti creando passaggi ed eseguendoli in modo autonomo, senza alcuna interfaccia con uomo.

SECTION

L' introduzione della A.I.
rischi e nuove minacce nel contesto etico

03



Le caratteristiche dell'AI espongono le organizzazioni a rischi nuovi.

GOVERNANCE

Sfide nell'allineare **visione aziendale e strategia AI**, e nel costruire una governance agile fatta di policy, processi, ruoli e responsabilità ben definiti.

COMPLIANCE Rischi legati al **rispetto di leggi, regolamenti** e policy, a livello nazionale ed europeo, sia nel mondo finanziario che tecnologico.

TECNOLOGIA

Rischi tecnici legati allo sviluppo di applicazioni di AI: **dalle performance insufficienti alla scarsa robustezza**, alla mancanza di interpretabilità e spiegabilità..

OPERATIONS Rischi legati alla mancanza di solide procedure di governance e controllo nei progetti di AI: **assenza di supervisione umana**, bassa trasparenza, scarsa tracciabilità e responsabilità poco definite.

SECURITY & DATA PROTECTION Rischi legati alla **sicurezza informatica, alla privacy e alla protezione dei dati**, sia per le applicazioni di AI che per i dati utilizzati e generati da esse.

SOSTENIBILITÀ

Impatti ambientali negativi legati all'elevato consumo di energia e risorse nello sviluppo dell'AI e delle infrastrutture tecnologiche, con rischi di **insostenibilità e danni reputazionali**.



I POSSIBILI NUOVI RISCHI IN DETTAGLIO -1

I software di A.I. avrebbero la possibilità di apprendere strategie efficaci, già adottate da altre macchine in situazioni analoghe, grazie ad un cloud comune, modificandole ed adattandole al caso concreto senza la necessità di un nuovo intervento del programmatore **grazie al cd. black box algorithms.**

Il pericolo insito nell'utilizzo dei software di valutazione del rischio, basati sulla programmazione prestabilita dal creatore, è quello che il sistema risponda predisponendo misure analoghe in contesti societari simili ma non identici, lasciando, aree vulnerabili ai rischi di commissione di reati.

L'imprevedibilità dell'auto-apprendimento, cd. machine learning, impedirebbe all'ente di governare e, in pratica, di indirizzare il software su, ad esempio, il bilanciamento tra procedure :

- ✓ di prevenzione
- ✓ maggior produttività
- ✓ rispetto della persona del complesso aziendale.

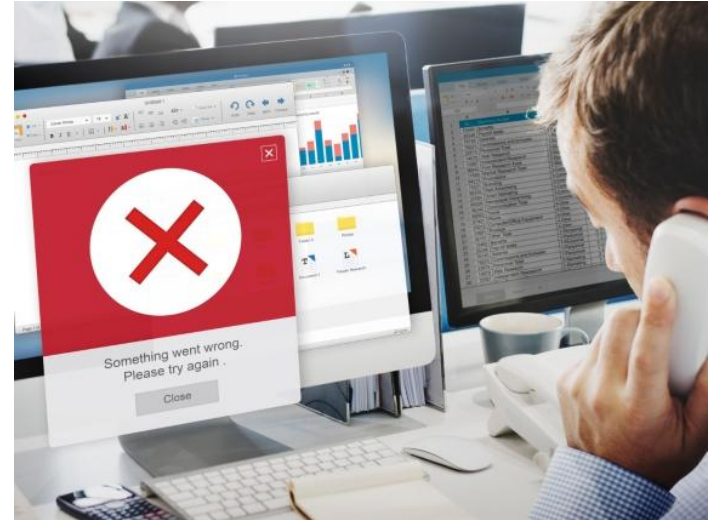


I POSSIBILI NUOVI RISCHI IN DETTAGLIO -2

Nuovi rischi legati alla possibilità che tali strumenti vengano utilizzati, anche inconsapevolmente, per la commissione di reati

- **condotte illecite** riconducibili a reati presupposto 231, quali il riciclaggio e l'autoriciclaggio le violazioni della proprietà intellettuale
- **la commissione di reati informatici**, che possono essere agevolati o direttamente commessi tramite tecnologie basate sull'intelligenza artificiale, quali l'accesso abusivo a sistemi informatici o telematici, il danneggiamento di sistemi informatici, la creazione di malware o l'impiego di chatbot malevoli capaci di ingannare utenti e carpire credenziali sensibili.
- **violazioni della normativa GDPR** in materia di protezione dei dati personali (GDPR), in particolare con riferimento alla raccolta massiva, al trattamento non conforme o alla profilazione automatizzata degli interessati.

L'APPELLO DI Yoshua Bengio



Se i Paesi non riescono a mettersi d'accordo su cosa fare con l'intelligenza artificiale, devono almeno **concordare su cosa l'AI non può fare.**

È la premessa di **un appello firmato da oltre duecento persone — tra cui nove ex capi di stato e dieci premi Nobel —** [presentato da Maria Ressa, premio Nobel per la pace, durante l'80esima sessione dell'Assemblea Generale dell'ONU.](#)

Tra i firmatari ci sono **Geoffrey Hinton e Yoshua Bengio**, pionieri e padri dell'intelligenza artificiale

L'iniziativa chiede un accordo globale entro la fine del 2026 su **linee rosse da non oltrepassare**



L'APPELLO dei massimi studiosi di AI



Stuart Russell, Ha fondato e dirige il *Center for Human-Compatible Artificial Intelligence* (CHAI) presso la citata UC, Berkeley e l'*International Association for Safe and Ethical Artificial Intelligence* (IASAI). Russell è coautore con [Peter Norvig](#) dell'autorevole libro di testo *Artificial Intelligence: A Modern Approach* (noto con l'acronimo AIMA) utilizzato in più di 1.500 università in 135 paesi. Docente di informatica all'Università di Berkeley, la vede così

Le aziende possono conformarsi «non costruendo l'intelligenza artificiale generale finché non sanno come renderla sicura... proprio come gli sviluppatori di energia nucleare non hanno costruito centrali nucleari finché non hanno avuto un'idea di come impedire loro di esplodere».

Yuval Noah Harari. Prof. Yuval Noah Harari is a historian, philosopher, and the bestselling author of *Sapiens: A Brief History of Humankind*, *Homo Deus*. His books have sold 50 Million copies in 65 languages.

E' ancora più netto: «Per migliaia di anni, gli esseri umani hanno imparato che le tecnologie potenti possono avere conseguenze tanto pericolose quanto benefiche. **Con l'AI, potremmo non avere la possibilità di imparare dai nostri errori, perché l'AI è la prima tecnologia che può prendere decisioni da sola, inventare nuove idee da sola, e sfuggire al nostro controllo».**

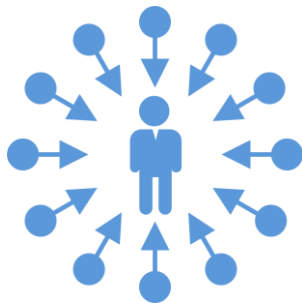


Human-in-the-Loop un altro elemento di rischio

Le aziende cercano di testare nuove tecnologie, ma spesso si rendono conto di un fattore cruciale: il ruolo degli esseri umani.

I lavoratori coinvolti nei processi produttivi, spesso dotati di conoscenza tacita, non accolgono l'automazione con lo stesso entusiasmo.

Progetti abbandonati al primo confronto con la realtà del lavoro umano.



Progettare soluzioni che mantengano l'essere umano al centro, secondo il principio human-in-the-loop, è essenziale per garantire non solo l'efficacia tecnica, ma anche il rispetto dei **valori umani e sociali**.

SECTION

Le nuove normative

04

Artificial Intelligence Act (AI Act) : IN EUROPA



L'Unione Europea ha approvato l'*Artificial Intelligence Act (AI Act)* ossia il regolamento (UE) 2024/1689 del 13 giugno 2024, con lo scopo di consentire:

1. lo sviluppo, la commercializzazione e l'utilizzo di strumenti di intelligenza artificiale all'interno dell'U E,
2. nel rispetto della sicurezza e dei diritti fondamentali dell'uomo.

L'art. 5 del Regolamento, rubricato “pratiche di AI vietate”, pone il divieto di utilizzo di alcune funzioni, ritenute potenzialmente lesive della sicurezza e dei diritti dell'Uomo. In particolare:

- è vietato l'utilizzo di **tecniche subliminali** o volutamente decettive, al fine di indurre le persone a prendere una decisione che altrimenti non avrebbe preso.
- Bisogna **tutelare il consenso informato** di ogni individuo, e non potranno essere utilizzati sistemi di intelligenza artificiale in modo fraudolento per indurre in errore i destinatari dell'informazione ad effettuare una scelta.



Artificial Intelligence Act (AI Act) – 3 note

Infine, con riguardo ai sistemi di identificazione biometrica remota “in tempo reale” utilizzabili in luoghi pubblici , **pone il medesimo divieto salvo che questo non sia essenziale per ricerca e prevenzione di reati particolarmente gravi .**

L'AI Act non può ovviamente essere applicata integralmente in un'unica soluzione. Le autorità europee hanno stabilito, a partire dall'entrata in vigore del 1° agosto 2024, **una serie di tappe regolamentari** distribuite nel tempo. Agosto 2026.

I fornitori e gli utilizzatori di sistemi di AI devono “formare il personale e delle altre persone che si occupano dell'esercizio e dell'uso dei sistemi di AI per loro conto” fino ad **un livello sufficiente di alfabetizzazione in materia di Intelligenza Artificiale**



LEGGE N°132 /2025

25-9-2025

GAZZETTA UFFICIALE DELLA REPUBBLICA ITALIANA

Serie generale - n. 223

LEGGI ED ALTRI ATTI NORMATIVI

LEGGE 23 settembre 2025, n. 132.

Disposizioni e deleghe al Governo in materia di intelligenza artificiale.

La Camera dei deputati ed il Senato della Repubblica hanno approvato;

IL PRESIDENTE DELLA REPUBBLICA

PROMULGA

principi di trasparenza, proporzionalità, sicurezza, protezione dei dati personali, riservatezza, accuratezza, non discriminazione, parità dei sessi e sostenibilità.

2. Lo sviluppo di sistemi e di modelli di intelligenza artificiale per finalità generali avviene su dati e tramite processi di cui devono essere garantite e vigilate la correttezza, l'attendibilità, la sicurezza, la qualità, l'appropriatezza e la trasparenza, secondo il principio di proporzionalità in relazione ai settori nei quali sono utilizzati.

Nella giornata del 25 settembre 2025, è stata pubblicata in Gazzetta Ufficiale la [Legge 23 settembre 2025 n. 132](#), con

“Disposizioni e deleghe al Governo in materia di Intelligenza Artificiale”, che è entrata in vigore il 10 ottobre.

La norma assegna delega al Governo affinché dia “*precisazione dei criteri di imputazione della responsabilità penale delle persone fisiche e amministrativa degli enti per gli illeciti inerenti a sistemi di Intelligenza Artificiale, che tenga conto del livello effettivo di controllo dei sistemi predetti da parte dell'agente*”.

La Legge apporta inoltre modifiche ad alcune fattispecie che rientrano nel Catalogo dei Reati Presupposto del DLGS 231/01”.

Si tratta dell'aggiotaggio (art. 2637 cc) e della manipolazione del mercato (art. 185 TUF) che si arricchiscono di una specifica aggravante per il caso in cui siano commessi mediante l'impiego di sistemi di Intelligenza Artificiale.



Ing. Relatore

[Commissione 231 seminario 6 Novembre 2025](#)

Data



Il parlamento italiano ha dato al governo 12 mesi per rilasciare un decreto legislativo per l'adeguamento della normativa nazionale all' AI Act

ITALIA – LEGGE SULL'INTELLIGENZA ARTIFICIALE



In data 17 settembre 2025 il Senato ha approvato in via definitiva la legge italiana sull'intelligenza artificiale («IA»),

L 132/2025, pubblicata nella GU n. 223 del 25.9.25 .

Si tratta del primo quadro normativo nazionale in Europa che disciplina sviluppo, adozione e governance dei sistemi di AI nel rispetto dei principi costituzionali e dei diritti fondamentali e in piena coerenza con l'AI Act europeo.

Entro 12 mesi il Governo dovrà adottare uno o più decreti legislativi per l'adeguamento della normativa nazionale all'AI Act.

Dati e ricerca.

Viene dato spazio all'**uso e al riuso dei dati personali e sanitari** ai fini di ricerca scientifica. Il trattamento viene riconosciuto come di **«rilevante interesse pubblico»**, ex art. 9.2, lett. g) del GDPR. Duque, gli obblighi di informativa verso i pazienti vengono semplificati, purché vengano adottate **misure di de-identificazione**.

Vigilanza e ispezioni.

Le autorità di mercato e di settore possono imporre obblighi informativi ai fornitori, **effettuare ispezioni anche senza preavviso** e controllare prove in condizioni reali per i sistemi ad alto rischio.

Governance aziendale.

Il quadro normativo richiederà un **rafforzamento dei ruoli interni** dedicati all'AI:

- nomina di responsabili della compliance AI;
- integrazione dei rischi AI nel *risk management* e nella reportistica al *board*;
- nuova attenzione alla gestione dei fornitori esterni.

Impatto sul lavoro.

Il **datore di lavoro** è tenuto a rispettare il vigente quadro in materia del diritto del lavoro, quindi l'art. 4 St. Lav. e il cd «Decreto Trasparenza» e dovrà **informare i lavoratori sull'uso dell'AI**; i sistemi devono rispettare la dignità e la riservatezza dei lavoratori e non discriminare. Viene anche istituito un **Osservatorio** presso il Ministero del Lavoro per monitorare l'impatto occupazionale, identificare i settori più esposti e promuovere la formazione.

Procurement e sovranità digitale.

Le pubbliche amministrazioni potranno privilegiare **soluzioni di AI con elaborazione dei dati strategici in data center localizzati su territorio nazionale**. Viene **eliminata** l'obbligatorietà della **clausola di localizzazione**.

Autorità competenti

L'Agenzia per la Cybersicurezza Nazionale (ACN) e l'Agenzia per l'Italia Digitale (AgID) sono individuate quali Autorità nazionali competenti: ACN esercita, anche mediante poteri ispettivi, la vigilanza sull'adeguatezza e sulla sicurezza dei sistemi, mentre AgID è responsabile della gestione delle notifiche e della promozione di casi d'uso sicuri a beneficio di cittadini e imprese, all'interno di un quadro di coordinamento interistituzionale stabile.



Legge 132/2025

La nuova legge rappresenta un momento fondamentale nella regolazione nazionale dell'intelligenza artificiale, colmando le lacune dell'AI Act europeo:

Introduce norme su AI e salute, tutela dei minori, coordinamento istituzionale e reati informatici.

Restano aperti i temi della

- **personalità elettronica**
- **dell'assicurazione obbligatoria**
- **della nuova figura professionale di controllo dell'AI**

L'art.26 della legge 132/2025 introduce il nuovo reato di Illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale prevedendo un nuovo articolo del codice penale, l'Art. 612 -quater;

L'articolo 26, inoltre, integra le previsioni dell'art. 2637 c.c in tema di "Aggiotaggio" prevedendo la pena della reclusione da due a sette anni se il fatto è commesso mediante l'impiego di sistemi di intelligenza artificiale.

Legge 132/2025 ed il DLGS 231/01



QUESTIONE

In caso di reato a seguito dell'applicazione di un Modello Gestionale prodotto da Gen AI, sulla base di input interni e data base disponibili in rete :

1. è possibile individuare gli input e gli output, ma non la catena causale che ha condotto dal dato originario al risultato finale.
2. Difficile applicazione dei tradizionali criteri di imputazione penale,
3. Difficile accertamento del nesso tra condotta umana ➡ evento dannoso

Responsabilità da reato degli enti. Se non è possibile configurare in capo alla persona fisica il reato presupposto, come potrebbe l'ente risponderne?

Art . 8 del d.lgs. 231, l'ente risponde anche quando l'autore del reato non sia stato identificato. Ma manca l'identificazione "apicale" dell'autore persona fisica.

Il Governo sulla base della L. 132/2025 dovrà definire i criteri di imputazione della responsabilità da reato delle persone fisiche e degli enti in relazione agli illeciti da intelligenza artificiale

SECTION

L' introduzione della A.I. nella
compliance

05



COMPLIANCE

Per esempio cerchiamo di comprendere le conseguenze dell'utilizzo di software *AI* nel settore della *compliance* aziendale, quindi la disciplina in tema di "colpa d'organizzazione" dell'ente.



Come si configura la responsabilità da colpa di organizzazione dell'ente che abbia affidato la gestione del proprio modello organizzativo e di gestione ad un *software AI*,



Indispensabile una dedicata **Risk Analysis** che prevede,

- ❖ definizione puntuale dei ruoli e responsabilità, dei processi,
- ❖ delle regole e dei divieti per l'adozione,
- ❖ l'utilizzo e l'acquisto di *AI*,
- ❖ un'attività di revisione ed eventuale aggiornamento degli stessi (es., Fastweb prevede una review e aggiornamento ogni 6 mesi).

AI Governance Per la mitigazione dei rischi, è fondamentale che le organizzazioni sviluppino un'adeguata AI Governance basata su più pilastri:

- **Policy e Procedure**

Implementare e continuamente aggiornare Linee guida, Policy e Procedure per garantirne compliance normativa ed etica.

- **Ruoli e responsabilità**

Definizione di ruoli e responsabilità, creando inoltre nuove posizioni per la gestione dei modelli di AI e lo sviluppo di competenze specifiche per l'AI.

- **Processi e controlli**

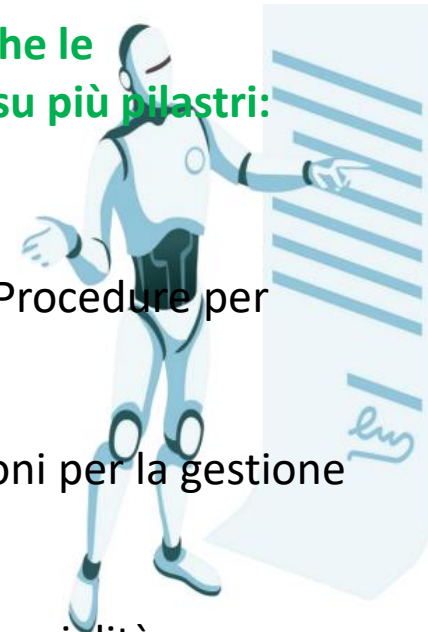
Predisporre processi e controlli volti a garantire l'affidabilità, l'imparzialità e l'accuratezza dei modelli di AI, ad esempio per la valutazione e approvazione degli «use case» con definizione di metodologie etiche per sviluppo, test e procurement.

- **Monitoring**

È necessario un monitoraggio costante dei processi di controllo interno, dei modelli di AI, dei rischi e degli «incidenti», per garantirne la conformità alle normative e agli standard etici. Inoltre, è fondamentale testare la qualità dei dati .

- **Comunicazione e formazione**

Una comunicazione chiara e una formazione mirata per assicurarsi che i dipendenti comprendano il ruolo dell'AI nell'organizzazione e come questa influenzi il loro lavoro.



Esempio di possibile applicazione pratica

Definizione ruoli e responsabilità



E l'ODV dove
si colloca in
questo
quadro ?

Funzione legale § compliance

- Analisi normativa vigente in materia AI
- Valutazione del sistema AI sul codice Etico
- Implementazione AI coerente rispetto le policy aziendali

Funzione IT :

- Test e verifiche tecniche sui sistemi AI
- Identificazione dei rischi di sicurezza informatica legati a AI

H.R.

- Formazione all'uso di AI

Funzione Approvvigionamenti

- Acquisto di nuovi modelli AI in linea con le esigenze aziendali

Comitato di Governance di AI

- Valutazione MULTIDISCIPLINARE di rischi ed opportunità delle iniziative AI
- Gestione errori e reclami
- Supervisione aggiornamento «policy e procedure»

Alfabetizzazione : Cosa prevede l' AI Act art. 4

L'articolo 4 dell'AI Act introduce **un obbligo specifico di garantire un adeguato livello di alfabetizzazione all'AI per il personale coinvolto nell'utilizzo dei sistemi di AI** (tutti, non solo quelli proibiti o ad alto rischio) Il regolamento impone infatti che fornitori e utilizzatori (deployer) di AI adottino misure per garantire che il personale rilevante, ossia che usa l'IA, abbia un "livello sufficiente di alfabetizzazione all'IA", tenendo conto del contesto e delle persone potenzialmente interessate dal sistema di AI in uso.

Nel regolamento dell'UE, la **nozione di "alfabetizzazione all'IA" è definita come il possesso delle competenze, conoscenze e comprensione adeguate per procedere ad una diffusione informata dei sistemi di AI** ed essere consapevoli delle opportunità e dei rischi associati all'AI.

La principale incognita è definire cosa si intende per un "livello sufficiente" di alfabetizzazione, previsto dal Regolamento.

Obblighi applicabili
dal 2 agosto 2025.



SECTION

RIASSUMENDO

06



Le implicazioni dell'Agentic AI in azienda

Chiunque abbia esperienze di lavoro in un'organizzazione può già immaginare le **opportunità**, ma anche i **rischi** e le **sfide** di quest'evoluzione tecnologica.

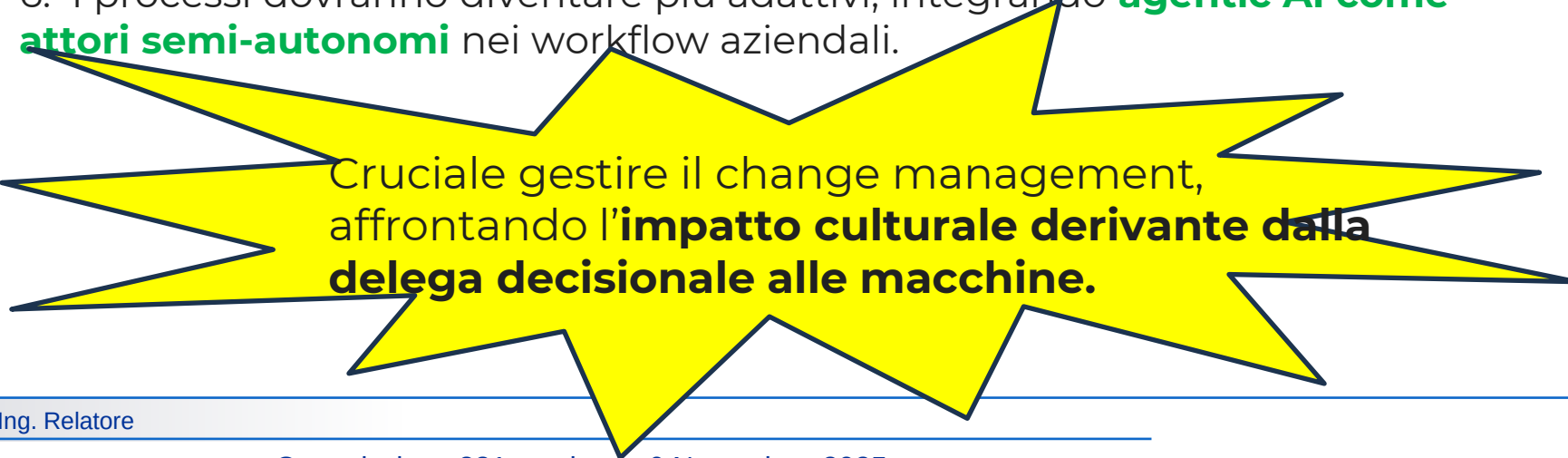
Restano infatti aperti diversi interrogativi fondamentali:

1. come garantire che gli **agentic AI agiscano nell'interesse degli utenti** e non sviluppino comportamenti indesiderati, assicurando un corretto allineamento degli obiettivi?
2. **chi sarà ritenuto responsabile** se un agente autonomo dovesse causare un danno, in un quadro di accountability ancora da definire?



Le implicazioni dell'Agentic AI in azienda

3. quali strategie saranno necessarie per **prevenire derive non intenzionali**, soprattutto in contesti critici come la finanza o la sanità?
4. Come debbano **cambiare le modalità di lavoro degli esseri umani** per ottenere vantaggio competitivo da questi strumenti : il cambiamento non sarà solo tecnologico, ma anche profondamente organizzativo.
5. Sviluppare nuove **skill, specializzati nella progettazione**, supervisione e “allenamento” degli agenti AI.
6. I processi dovranno diventare più adattivi, integrando **agentic AI come attori semi-autonomi** nei workflow aziendali.



Cruciale gestire il change management, affrontando l'**impatto culturale derivante dalla delega decisionale alle macchine.**



Researchers claim
**humans with AI won't replace people,
but its users
might replace those who don't use it.**

Relatore

Ing ROBERTO FRANCINI 3332214541

SECTION

BACK UP

06



INTELLIGENZA ARTIFICIALE E PRINCIPI DELLA PROTEZIONE DEI DATI

Requisiti per la protezione dei dati	TENSIONI DA RISOLVERE	Intelligenza Artificiale
Base giuridica del trattamento		Il trattamento a monte dei dati può non essere sostenibile e la varietà di basi giuridiche disponibili è insufficiente/limitata
Consenso		Un comportamento autonomo e adattabile può richiedere un trattamento imprevedibile dei dati a valle
Minimizzazione dei dati		Richiede un accesso ampio e dinamico a grandi quantità di dati per svolgere compiti complessi
Finalità specifiche e limitazioni		Utilizza i dati per scopi nuovi e imprevisi al di là dello scopo originario
Trasparenza		Un processo decisionale non lineare e adattivo può portare a risultati inspiegabili e non previsti
Limitazione della conservazione		Gli agenti devono memorizzare e riutilizzare i dati per migliorare le prestazioni nel tempo
Diritti individuali		Difficile agevolare l'accesso, la correzione, la cancellazione o la spiegazione della logica coinvolta
Regole sul processo decisionale automatizzato (PDA)		Il PDA è inerente all'IA, ma potrebbe essere necessario limitarlo a decisioni non legali o non significative
Restrizioni al trasferimento transfrontaliero dei dati		Necessità di utilizzare dati diversi e geograficamente dispersi