AODV – Il processo di compliance integrato e il MOG231 alla prova dell'Intelligenza Artificiale: punti di contatto e frizioni con il GDPR –

Avv. Francesca Gravili – Head of Data Protection & New Tech

Milano 7 ottobre 2025

I RISCHI CONNESSI ALL'USO DELL'AI

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.

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.

ITALIA – LEGGE SULL'INTELLIGENZA ARTIFICIALE

Impatti «231» della Legge sull'intelligenza artificiale

Deleghe al Governo

«*Il Governo è delegato ad adottare entro dodici mesi dalla data di entrata in vigore della presente 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 [….] Il Governo si attiene ai seguenti princìpi e criteri direttivi:*

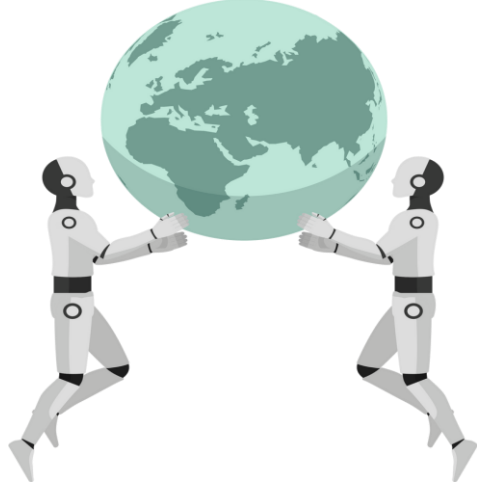
- *b) **introduzione** di **autonome fattispecie di reato,** punite a titolo di dolo o di colpa, incentrate sull'**omessa adozione o sull'omesso adeguamento di misure di sicurezza per la produzione, la messa in circolazione e l'utilizzo professionale di sistemi di intelligenza artificiale**, quando da tali omissioni deriva pericolo concreto per la vita o l'incolumità pubblica o individuale o per la sicurezza dello Stato;*
- *c) **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*».

Impatto sui reati presupposto 231

Introdotte **aggravanti «*se il fatto è commesso mediante l'impiego di sistemi di intelligenza artificiale*»** ai reati di:

- **aggiotaggio (art. 2637 c.c.)**
- **manipolazione del mercato (art. 185 TUF).**

I pilastri dell'AI Governance



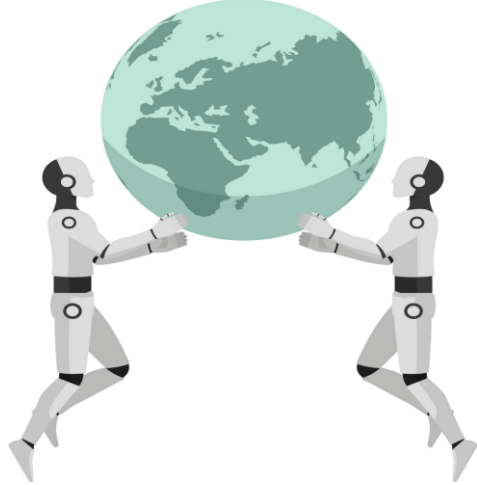
AI Governance e 231

L'adozione di tecnologie basate su IA può generare:

- 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 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.

I pilastri dell'AI Governance

AI Governance e 231



Il Modello organizzativo 231
deve essere rivisto e strutturato in considerazione di tali nuove aree di rischio?

I) Partiamo dalla mappatura dei sistemi di AI.

Artificial Intelligence Act («AI ACT»)

1. Mappatura dei sistemi di AI

WHAT TO DO

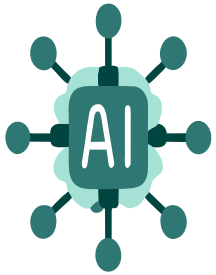
Le aziende sono chiamate a verificare se i Sistemi informatici impiegati nei propri processi aziendali o nelle attività quotidiane rientrano nella definizione di "**sistema di IA**" riportata nell'art. 3 dell'AI Act.

> *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.*

HOW TO DO

Effettuando una **mappatura completa dei sistemi di Intelligenza Artificiale** (IA) utilizzati, al fine (anche) di identificare quelli che potrebbero rientrare nelle categorie ad alto rischio o vietate.
(il 29 luglio 2025 la Commissione ha definitivamente pubblicato: "*Orientamenti della Commissione relativi alle pratiche di intelligenza artificiale vietata ai sensi del regolamento (UE) 2024/1689)*".

I pilastri dell'AI Governance

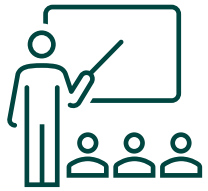


AI Governance e 231

Il Modello organizzativo 231
deve essere rivisto e strutturato in considerazione di tali nuove aree di rischio?

II) Parliamo di ALFABETIZZAZIONE

ALFABETIZZAZIONE IN MATERIA DI AI E RELATIVI DOCUMENTI



COS'È L'ALFABETIZZAZIONE?

L'alfabetizzazione in materia di **Intelligenza Artificiale** è un **obbligo** introdotto **dall'art. 4 del Regolamento (UE) 2024/1689 («AI ACT»),** rivolto sia ai **produttori** sia agli **utilizzatori** dei sistemi di AI, che consiste nella **formazione** finalizzata a garantire la **comprensione chiara e consapevole**:

- di che **cosa sia un sistema di Intelligenza Artificiale**;
- del suo **funzionamento**;
- dei **rischi e delle opportunità** connessi al suo impiego;
- delle modalità per **utilizzarlo responsabilmente**.

DOCUMENTI

La **Commissione Europea** ha pubblicato due documenti volti a supportare l'implementazione dell'Art. 4 dell'AI Act:

1. il ***Living Repository of AI Literacy Practices***;
2. l'***Ai Literacy – Questions & Answers***.

OBIETTIVO

Assicurare «le competenze, le conoscenze e la comprensione che consentono ai **fornitori, ai deployer e alle persone interessate**, […] di procedere a una **diffusione informata** dei sistemi di AI, nonché di **acquisire consapevolezza** in merito alle **opportunità** e ai **rischi** dell'AI e ai **possibili danni** che essa può causare» (art. 3, n. 56 dell'AI Act).

Alfabetizzazione in materia di AI

I fornitori e i deployer dei Sistemi di AI adottano misure per ***garantire*** *nella misura del possibile* ***un livello sufficiente di alfabetizzazione in materia di AI del loro personale nonché di qualsiasi altra persona che si occupa del funzionamento e dell'utilizzo dei Sistemi di AI per loro conto****, prendendo in considerazione le loro conoscenze tecniche, la loro esperienza, istruzione e formazione, nonché il contesto in cui i sistemi di AI devono essere utilizzati, e tenendo conto delle persone o dei gruppi di persone su cui i sistemi di AI devono essere utilizzati.*

OBIETTIVO

- Assicurare un livello adeguato di conoscenza sui Sistemi di AI per il personale e gli utilizzatori.
- Predisporre adeguati piani formativi sulla base dell'esperienza, dell'istruzione e del contesto d'utilizzo.

RISCHI

I dipendenti **non comprendono il funzionamento dei Sistemi di AI** e non sono formati sulle misure di mitigazione, il che potrebbe aumentare notevolmente i rischi di non conformità all'AI Act.

COSA POSSONO FARE LE ORGANIZZAZIONI

- Predisporre **programmi di formazione** per il personale (ad es. sulle procedure adottate o sul processo da seguire in caso di acquisto di un nuovo Sistema) e prevedere **aggiornamenti formativi** periodici ogniqualvolta ciò si renda necessario;
- Garantire un **monitoraggio costante** della normativa e delle eventuali evoluzioni dei Sistemi.

REPERTORIO DI PRATICHE SULL'ALFABETIZZAZIONE IN MATERIA DI AI

La Commissione Europea ha pubblicato, in data 28 marzo 2025, il **Repertorio di pratiche sull'alfabetizzazione in materia di Intelligenza Artificiale** (***Living Repository of AI Literacy Practices***), un insieme di ***best practices*** volto a supportare l'implementazione dell'Art. 4 dell'AI Act.

ALCUNE PRATICHE ATTUATE DA ORGANIZZAZIONI DI VARIE DIMENSIONI

Una formazione differenziata, a seconda del:

- **livello base**, accessibile a tutti, quindi generale su AI e governance AI aziendale;
- **livello intermedio** e **avanzato** in base al livello di coinvolgimento del dipendente con i sistemi AI, quindi più specifica;
- **contenuto**, organizzato in base alla complessità tecnica.

Una formazione diversificata, ossia:

caratterizzata da percorsi formativi con contenuti in **formato diversificato** e **inclusivo** (es., video, podcast, storytelling, che consente di simulare scenari realistici e favorire l'apprendimento esperienziale e pratico dell'uso dei dati e dell'AI, programmi di e-learning).

Un Modello di governance dell'AI:

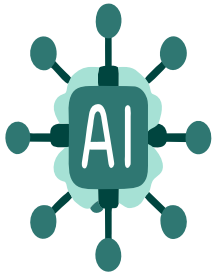
finalizzato non solo ad identificare il ruolo della società e il livello di rischio del sistema di AI secondo l'AI ACT, ma anche a **tener conto dell'impatto del sistema rispetto ad un quadro normativo più ampio** (es., impatto sui dati personali, sul copyright, sull'ESG, ecc.).

Un Risk Assessment che:

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

I pilastri dell'AI Governance

AI Governance e 231



Il Modello organizzativo 231
deve essere rivisto e strutturato in considerazione di tali nuove aree di rischio?

Questi scenari impongono alle imprese un'attenta riflessione sull'integrazione dell'IA nei processi aziendali, richiedendo l'adozione di misure organizzative e tecniche adeguate a prevenire responsabilità dirette e indirette derivanti dall'uso delle nuove tecnologie.

III) Parliamo AI Governance

Esempi di applicazione pratica

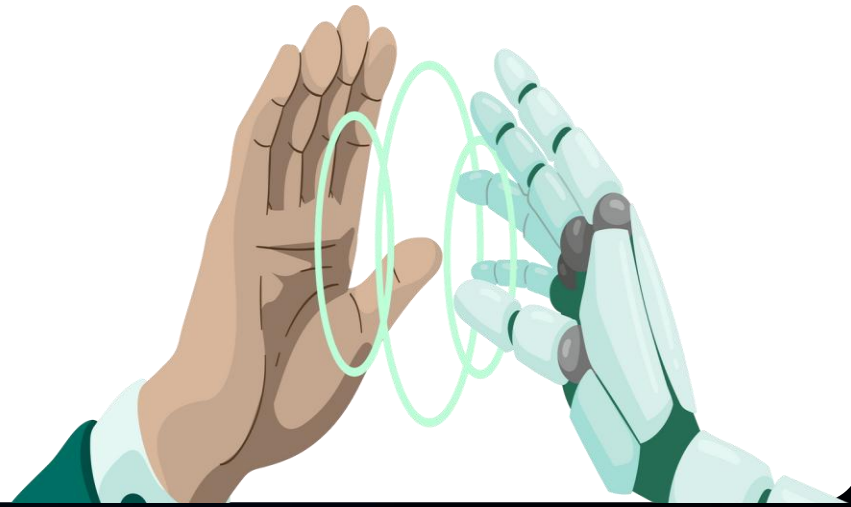
Esempio di «Policy per l'utilizzo dell'Intelligenza Artificiale»

Obiettivi:

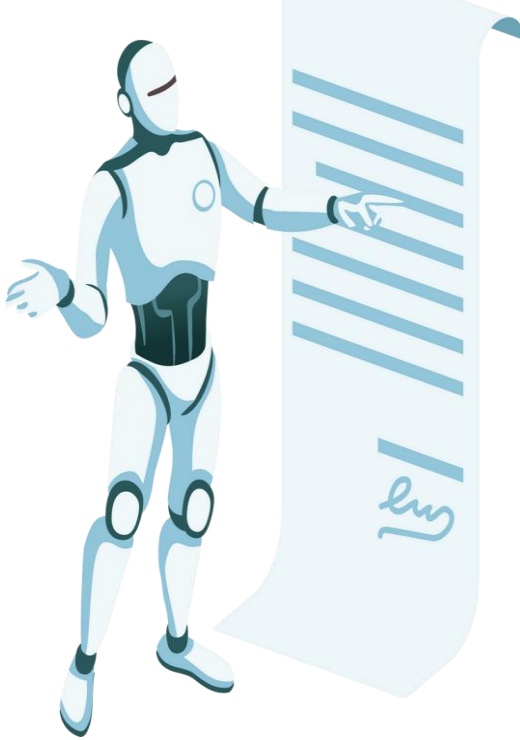
- Definire le linee guida per un utilizzo efficace, consapevole ed etico degli strumenti e sistemi di AI
- Stabilire i principi generali di utilizzo «responsabile» dei modelli di AI adottati
- Delineare i ruoli e responsabilità degli attori coinvolti

Elementi chiave:

- Definizione di un elenco degli strumenti di AI approvati/autorizzati, classificazione dei modelli sulla base dei livelli di rischio e relativi use case
- Workflow interno per la proposta e la valutazione di nuovi strumenti e sistemi di AI
- Processo di gestione dello sviluppo, addestramento e testing dei modelli di AI
- Gestione e risposta di «incidenti» e malfunzionamenti legati all'utilizzo di sistemi di AI
- Regole per la protezione della proprietà intellettuale, dei dati personali e tutela della privacy
- Programmi di formazione e sensibilizzazione



I pilastri dell'AI Governance



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**

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 per assicurare l'affidabilità e l'accuratezza dei modelli

- **Comunicazione e formazione**

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

Esempi di applicazione pratica

Esempio di definizione di ruoli e responsabilità

E L'ODV?

- **Funzione Legale & Compliance:**
  - analisi delle normative vigenti a livello nazionale e internazionale in materia di AI
  - valutazione degli effetti dei sistemi AI sulla conformità legale e sull'aderenza ai principi etici (Codice Etico)
  - assicurare che l'implementazione delle iniziative AI siano coerenti rispetto alle policy

FLUSSI?

- **Funzione IT:**
  - test e verifiche sui sistemi AI
  - identificazione dei rischi di sicurezza informatica legati all'uso dell'AI

- **Funzione Risorse Umane:**
  - attività di formazione sull'uso responsabile dell'AI

- **Funzione Approvvigionamenti:**
  - valutazione e acquisto di modelli di AI in linea con le esigenze aziendali

- **Comitato di Governance dell'AI:**
  - valutazione in modo multidisciplinare di rischi e opportunità delle iniziative AI, considerando aspetti tecnici, economici, legali ed etici
  - gestione di reclami e segnalazioni legate all'AI
  - supervisione dell'implementazione e aggiornamento di policy e procedure in ambito AI

EDPB – IA ADEGUATA AL GDPR

STEPS PRATICI PER LE AZIENDE CHE IMPLEMENTANO MODELLI DI IA

Predisporre DPIA periodiche, identificando le aree ad alto rischio e rivedere le valutazioni in concomitanza all'evoluzione dei modelli.

Scegliere e documentare idoneamente le basi giuridiche, ricordando che l'interesse legittimo richiede un accurato *balancing test*.

Implementare tecniche privacy adeguate: anonimizzazione e pseudonimizzazione possono ridurre i rischi di re-identificazione.

Mantenere una documentazione dettagliata.

Testare le vulnerabilità: valutare regolarmente il modello di IA contro minacce come gli attacchi di inferenza di appartenenza, l'inversione del modello e altri potenziali exploit.

Garantire la trasparenza: assicurarsi che gli interessati sappiano come vengono utilizzati i loro dati, quali diritti hanno e specificare che si tratta di sistemi di IA.

Rimanere informati: seguire gli aggiornamenti normativi e l'evoluzione best practices del settore.

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 imprevisti 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