



# **IA**

# **Mog 231, GDPR**

# **e cybersicurezza**

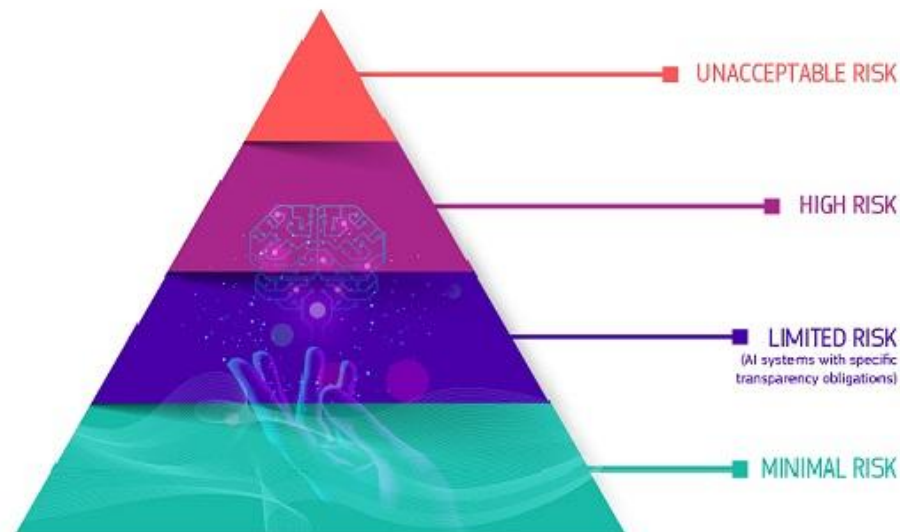
**a cura di**  
**Roberto Scavizzi**  
**docente universitario e avvocato del foro di Roma**



# AI → 'Risk based Thinking'

Il quadro normativo definisce 4 livelli di rischio nell'IA\*:

- ✓ Rischio *inaccettabile*
- ✓ Rischio *elevato*
- ✓ Rischio *limitato*
- ✓ Rischio *minimo o nullo*



\*[digitalstrategy.ec.europa.eu/it/policies/regulatory-framework](https://digitalstrategy.ec.europa.eu/it/policies/regulatory-framework)



# High Risk AI Systems

*How does it all work in practice for providers of high risk AI systems?*





# Il Libro Bianco sull'intelligenza artificiale

L'UE sull'*intelligenza artificiale* ritiene che si debba adottare *un approccio europeo all'eccellenza e alla fiducia per un AI ANTROPOCENTRICA*



# I sette requisiti fondamentali dell' IA

La Commissione ha pubblicato una comunicazione in cui accoglie con favore *i sette requisiti fondamentali* individuati negli orientamenti del gruppo di esperti ad alto livello:

- ✓ *intervento e sorveglianza umani*
- ✓ *robustezza tecnica e sicurezza*
- ✓ *riservatezza e governance dei dati*
- ✓ *trasparenza*
- ✓ *diversità, non discriminazione ed equità*
- ✓ *benessere sociale e ambientale*
- ✓ *accountability.*



# Le cd '*distorsioni*'

Le distorsioni e le discriminazioni rappresentano ***un rischio intrinseco*** di qualunque attività sociale od economica.

Il processo decisionale umano non è immune da errori e distorsioni.



# L'effetto '*scatola nera*'

Le caratteristiche specifiche di molte tecnologie di IA, tra cui *l'opacità* (*effetto 'scatola nera'*), la *complessità*, *l'imprevedibilità* e un *comportamento parzialmente autonomo*, possono rendere difficile verificare il rispetto delle normative dell'UE in vigore volte a proteggere i diritti fondamentali e possono ostacolarne l'applicazione effettiva.



# Cos'è un sistema di IA? (Art. 3)

«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»;



# Alfabetizzazione in materia di IA

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



# PRATICHE VIETATE



Relatore : avv. Roberto Scavizzi

Commissione 231 seminario 6

Novembre 2025

Data



# Inferire emozioni

l'immissione sul mercato, la messa in servizio per tale finalità specifica o l'uso di sistemi di IA per **inferire le emozioni di una persona fisica nell'ambito del luogo di lavoro** e degli istituti di istruzione, **tranne** laddove l'uso del sistema di IA sia destinato a essere messo in funzione o immesso sul mercato **per motivi medici o di sicurezza**;



# Categorizzazione biometrica

**l'immissione sul mercato, la messa in servizio per tale finalità specifica o l'uso di sistemi di categorizzazione biometrica che classificano individualmente le persone fisiche sulla base dei loro dati biometrici per trarre deduzioni o inferenze in merito a razza, opinioni politiche, appartenenza sindacale, convinzioni religiose o filosofiche, vita sessuale o orientamento sessuale;**



# **ALLEGATO III**

## **Sistemi di IA ad alto rischio di cui all'articolo 6, paragrafo 2 dell'AI Act**



# Lista dei sistemi IA ad '*alto rischio*'

I sistemi di IA ad alto rischio a norma dell'articolo 6, paragrafo 2 dell'AI

**Act, sono** i sistemi di IA elencati in uno dei settori indicati di seguito.



# Occupazione e lavoro

## Occupazione, gestione dei lavoratori e accesso al lavoro autonomo:

- a. i sistemi di IA destinati a essere utilizzati per l'assunzione o la selezione di **persone fisiche**, in particolare per pubblicare annunci di lavoro mirati, analizzare o filtrare le candidature e valutare i candidati;
- b. i sistemi di IA destinati a essere utilizzati per adottare decisioni riguardanti le condizioni dei rapporti di lavoro, la promozione o cessazione dei rapporti contrattuali di lavoro, per assegnare compiti sulla base del comportamento individuale o dei tratti e delle caratteristiche personali o per monitorare e valutare le prestazioni e il comportamento delle persone nell'ambito di tali rapporti di lavoro.



# **Applicazione dell'IA al settore della sicurezza sul lavoro**



Relatore : avv. Roberto Scavizzi

Commissione 231 seminario 6  
Novembre 2025

Data



# H&S e la tecnologia

Le tecnologie di automazione hanno aggiunto ulteriore complessità all'organizzazione.

L'interazione delle 'macchine' con l'uomo, infatti, richiede alle aziende di prestare ancora più attenzione all' *Health&Safety* negli ambienti industriali.



# Localizzazione in tempo reale

Tuttavia, le tecnologie offrono anche un supporto alle imprese ai fini della tutela della salute e sicurezza dei lavoratori e della conformità alle normative vigenti.

È il caso delle tecnologie dell'IoT (*Internet of Things*) e, in particolare, dei **sistemi di localizzazione in tempo reale (RTLS)**, che **aiutano a ridurre notevolmente il rischio di incidenti**.



# ***IoT***

Le tecnologie dell'***Internet of Things*** sono sempre più diffuse negli ambienti industriali.

La possibilità di ***monitorare costantemente dati relativi agli ambienti produttivi e ai macchinari*** permette, infatti, di gestire l'impianto e tutti i processi in modo più efficiente.



# ***IoT e RTLS***

Mediante un'integrazione delle soluzioni basate sull'*Internet of Things* industriale con i dispositivi RTLS (cd '*Real-Time Locating System*') si possono conseguire miglioramenti concreti nel funzionamento dell'organizzazione.

Invero, mediante ***l'utilizzo di detti dispositivi è possibile localizzare (direttamente e indirettamente) e tracciare operatori, macchinari e oggetti.***



# Tracciamento massivo

**I dispositivi RTLS si servono di variegate tecnologie (*Bluetooth, GPS o Ultra wideband*) per rilevare la posizione di operatori e macchinari all'interno delle aree aziendali.**

**L'utilizzo di tali dispositivi consente il tracciamento in tempo reale e senza interruzioni di operatori e macchine per l'intera giornata lavorativa.**



# *Privacy degli operatori*

Il tracciamento diretto degli operatori mediante i prefati dispositivi consente di ***migliorare la salute e sicurezza dei lavoratori negli ambienti di lavoro.***

**Tale obiettivo deve essere perseguito nel pieno rispetto della privacy degli operatori.**

In tal senso i dispositivi in esame potrebbero consentire il controllo del lavoratore in merito al corretto utilizzo (es: se lo indossa oppure no; se lo indossa correttamente; se i suoi parametri vitali sono in regola, etc) dei dispositivi di protezione individuale o alla verifica del suo stato di salute.



# Utilizzo *RTLS*

Inoltre, queste tecnologie sono in grado di **ottimizzare e razionalizzare la gestione degli spazi dell'organizzazione.**

Ad esempio ***detti dispositivi consentono di gestire e regolare gli accessi a determinate aree dell'impresa*** senza la necessità di ricorrere a barriere fisiche.

***Tale scelta tecnologico/organizzativa consente una più rapida ed efficace assistenza dei lavoratori/operatori in caso di incidenti (si pensi ai lavoratori che operano in solitario).***

Tali dispositivi prevedono l'invio bidirezionale di allarmi, segnalazioni e chiamate.



# **Alcune riflession sull'*AI Act***



Relatore : avv. Roberto Scavizzi

Commissione 231 seminario 6 Novembre 2025

Data



# Monitoraggio e tracciamento

In relazione ai sistemi di IA ad alto rischio è istituito, attuato, documentato e mantenuto un sistema di gestione dei rischi.



# Il Sistema di gestione dei rischi

L'operatore infortunato che rimane cosciente può utilizzare il dispositivo RTLS per richiedere soccorso.

Tali sistemi consentono di aumentare il livello di sicurezza anche per quegli operatori che operano in solitario e in aree isolate.



# La governance dei dati

I sistemi di IA ad alto rischio che utilizzano tecniche che prevedono l'uso di dati per l'addestramento di modelli di IA sono sviluppati sulla base di set di dati di addestramento, convalida e prova che soddisfano determinati criteri di qualità.



# La documentazione tecnica

La documentazione tecnica di un sistema di IA ad alto rischio è redatta prima dell'immissione sul mercato o della messa in servizio di tale sistema ed è tenuta aggiornata.



# ***Logging***

I sistemi di IA ad alto rischio consentono a livello tecnico la registrazione automatica degli eventi («log») per la durata del ciclo di vita del sistema.



# La trasparenza

I sistemi di IA ad alto rischio sono progettati e sviluppati in modo tale da garantire che il loro funzionamento sia sufficientemente trasparente da consentire ai *deployer* di interpretare l'output del sistema e utilizzarlo adeguatamente.

Sono garantiti un tipo e un livello di trasparenza adeguati, che consentano di conseguire il rispetto dei pertinenti obblighi del fornitore e del *deployer*



# La trasparenza '*adeguata*'

I sistemi di IA ad alto rischio sono progettati e sviluppati in modo tale da garantire che il loro funzionamento sia sufficientemente trasparente da consentire ai *deployer* di interpretare l'output del sistema e utilizzarlo adeguatamente.

Sono garantiti un tipo e un livello di trasparenza adeguati, che consentano di conseguire il rispetto dei pertinenti obblighi del fornitore e del *deployer*



# La sorveglianza umana

I sistemi di IA ad alto rischio sono progettati e sviluppati, anche con strumenti di interfaccia uomo-macchina adeguati, in modo tale da poter essere efficacemente supervisionati da persone fisiche durante il periodo in cui sono in uso.



# Accuratezza, robustezza

I sistemi di IA ad alto rischio sono progettati e sviluppati in modo tale da conseguire un adeguato livello di accuratezza, robustezza e ciphersicurezza e da operare in modo coerente con tali aspetti durante tutto il loro ciclo di vita.

I livelli di accuratezza e le pertinenti metriche di accuratezza dei sistemi di IA ad alto rischio sono dichiarati nelle istruzioni per l'uso che accompagnano il sistema.

I sistemi di IA ad alto rischio sono ***il più resilienti possibile*** per quanto riguarda errori, guasti o incongruenze che possono verificarsi all'interno del sistema o nell'ambiente in cui esso opera, in particolare a causa della loro interazione con persone fisiche o altri sistemi.

A tale riguardo sono adottate misure tecniche e organizzative.



# I doveri del *Deployer*

I *deployer* di sistemi di IA ad alto rischio adottano idonee misure tecniche e organizzative per garantire di utilizzare tali sistemi conformemente alle istruzioni per l'uso che accompagnano i sistemi

I *deployer* affidano la sorveglianza umana a persone fisiche che dispongono della competenza, della formazione e dell'autorità necessarie nonché del sostegno necessario.



# I doveri del *deployer*-datore di Lavoro è [1/2]

Sul punto la dottrina\* ha osservato quanto segue:

«Cosa dovrà fare quindi il **deployer – datore di lavoro** per agire correttamente ai sensi del Regolamento IA, qualora intendesse utilizzare l'IA per finalità definite ad alto rischio?

Il considerando 93 definisce cruciale il ruolo dei **deployer** che utilizzano sistemi IA ad alto rischio al fine di informare le persone fisiche che sono soggette all'uso di tali sistemi IA.

Sarà poi l'articolo 26 dell'AI Act a descriverne i principali obblighi generali.

Innanzitutto il comma 7 dell'articolo 26, stabilisce che **prima di mettere in servizio o utilizzare un sistema di IA ad alto rischio sul luogo di lavoro, i datori di lavoro informano i rappresentanti dei lavoratori e i lavoratori interessati che saranno soggetti all'uso del sistema di IA ad alto rischio.**

Oltre a dare preventiva informazione, sono previste ulteriori regole generali incluse anche in altri passaggi del Regolamento IA oltre che all'articolo 26, ossia e **in sintesi:**

- i. **un uso conforme** alle istruzioni del fornitore e adozione di adeguate misure tecniche e organizzative per l'uso corretto del sistema (art. 26);
- ii. **la sorveglianza umana adeguata** poiché eventuali decisioni automatizzate dovranno comunque essere supervisionate da persone fisiche (art. 14)»\*

\*In [agendadigitale.eu/industry-4-0/lavoratori-controllati-con-lai-cosa-prevede-lai-act-e-le-sinergie-col-gdpr](https://agendadigitale.eu/industry-4-0/lavoratori-controllati-con-lai-cosa-prevede-lai-act-e-le-sinergie-col-gdpr)



# I doveri del *deployer*-datore di Lavoro è [2/2]

- iii. **«il personale** che accede ai sistemi IA e che lo utilizza per conto del deployer dovrà avere **la formazione e le competenze necessarie** per un utilizzo corretto (art. 29)
- iv. **l'effettuazione di una notifica al fornitore e/o alle Autorità competenti**, a seconda dei casi, tra cui quella del Garante per la protezione dei dati, in caso di anomalie gravi o incidenti informatici (art. 73);
- v. **la conservazione dei log generati dal sistema per almeno 6 mesi**, salvo diverse disposizioni nazionali (art. 12 e 29) e
- vi. **una valutazione di impatto sui diritti fondamentali**, predisposta secondo le previsioni dell' articolo 35 del Gdpr (art. 29). Perciò tale valutazione dovrà essere effettuata prima dell'avvio dell'utilizzo del sistema di intelligenza artificiale, come previsto dal citato articolo e rivisita in caso di modifiche del sistema IA.

Infine, ai sensi dell'articolo 49, **i deployer – datori di lavoro soggetti pubblici, dovranno altresì prima dell'utilizzo di un sistema IA registrarsi, indicare il sistema IA utilizzato e registrarne l'uso in una banca dati europea istituita ad hoc ai sensi dell'articolo 71»\***.

\* In [agendadigitale.eu/industry-4-0/lavoratori-controllati-con-lai-cosa-prevede-lai-act-e-le-sinergie-col-gdpr](https://agendadigitale.eu/industry-4-0/lavoratori-controllati-con-lai-cosa-prevede-lai-act-e-le-sinergie-col-gdpr)



# Lo statuto dei lavoratori

«L'articolo 4 dello Statuto dei lavoratori che nella versione novellata dal Job Act impone il rispetto della normativa in materia di trattamento di dati, **vieta l'uso di strumenti di controllo a distanza, salvo previo accordo sindacale o autorizzazione dell'Ispettorato del Lavoro competente**, fermo restando che tali mezzi di controllo debbano essere impiegati esclusivamente per finalità relative ad esigenze organizzative e produttive, **per la sicurezza del lavoro** e per la tutela del patrimonio aziendale e solo in tali casi ci si potrà rifare al concetto di interesse legittimo del titolare (art. 6 comma 1 lett. f) quale base giuridica per le finalità di trattamento citate»\*.

\* In [agendadigitale.eu/industry-4-0/lavoratori-controllati-con-lai-cosa-prevede-lai-act-e-le-sinergie-col-gdpr](https://agendadigitale.eu/industry-4-0/lavoratori-controllati-con-lai-cosa-prevede-lai-act-e-le-sinergie-col-gdpr)



# Le *‘criticità’* in tema di *privacy* [1/3]

*Un sistema di rilevamento della posizione molto accurato* consente a siffatti sistemi di calcolare e rilevare con estrema precisione, accuratezza ed in tempo reale la distanza tra due veicoli o tra un veicolo e l'operatore.

Quando questa distanza si riduce, sia il dispositivo presente sul veicolo che quello di cui è dotato l'operatore segnalano il pericolo.

Se la distanza viene ulteriormente ridotta, il sistema può addirittura intervenire per ridurre la velocità del mezzo.

Ciò, naturalmente, comporta una serie di *‘criticità’* sul piano della corretta applicazione della normativa a tutela della privacy del lavoratore (art. 4 Statuto Lavoratori in combinato disposto con il GDPR) e dell'IA Act



# Le *'criticità'* in tema di *privacy* [2/3]

«I sistemi RTLS includono, oltre ai dispositivi, anche software di localizzazione che utilizzano i dati raccolti dai dispositivi per fornire delle informazioni strategiche.

Tra queste può esserci, ad esempio, ***l'analisi della composizione di una squadra di lavoro o l'inventario dei mezzi di movimentazione presenti nell'impianto***».

Mediante detti sistemi «l'azienda può analizzare i flussi di transito nelle diverse aree dello stabilimento per ridisegnare gli spazi in un'ottica di maggiore sicurezza ed efficienza»\*.

\* In [ubiquicom.com](http://ubiquicom.com)



# Le *'criticità'* in tema di *privacy* [3/3]

Egualemente le medesime riflessioni possono essere fatte relativamente ai rapporti aventi ad oggetto i cd *'near-miss'*, cioè a dire i *'quasi incidenti'*.

Dalla rilevazione e dal tracciamento di detti eventi è possibile poi individuare ***zone 'critiche' dell'impresa*** al fine di intervenire con modifiche tempestive dell'architettura organizzativa e aiutare l'azienda a intervenire prima che si verifichi un incidente.



# Il monitoraggio di molestie nell'ambiente di lavoro

Oltre a monitorare i lavoratori dipendenti, ***i sistemi di IA consentono anche di monitorare eventuali molestie***, le quali rappresentano un problema piuttosto grave all'interno delle organizzazioni.



# La riduzione degli errori umani: *profili privacy...*



**La possibilità di ridurre gli errori umani:** molto spesso, la causa degli infortuni o degli incidenti sul luogo di lavoro sono proprio gli errori umani, i quali sono a loro volta causati dalla stanchezza e dallo stress a cui spesso i lavoratori sono esposti.



**I sistemi di IA** sono efficaci anche in questo senso, dal momento che possono rilevare la stanchezza dei lavoratori e, conseguentemente, inviare dei segnali che li avvisino del potenziale pericolo, prima che gli infortuni o gli incidenti si verifichino in maniera effettiva.



# Sicurezza sul lavoro, IA e *privacy* [1/2]

Un altro modo per garantire la sicurezza sul lavoro con l'intelligenza artificiale è con i sistemi di riconoscimento delle immagini e degli oggetti.

Di seguito alcune ***delle numerose possibili applicazioni:***

- ✓ **Monitorare i flussi delle persone in siti industriali, magazzini, uffici, cantieri edili, centri logistici.** E' possibile addestrare un software di riconoscimento facciale a estrapolare i volti da riprese video in tempo reale, per poi confrontare i tratti biometrici con quelli inseriti in determinate categorie di un database, in modo da consentire solamente al personale autorizzato di entrare nelle aree con restrizioni di accesso.



# Sicurezza sul lavoro, AI e *privacy* [2/2]

- ✓ **Assistere i conducenti nella guida di veicoli tramite il rilevamento biometrico di espressioni facciali** che caratterizzano stati fisici come sonnolenza e distrazione, diminuendo così la probabilità che avvengano incidenti.
- ✓ **Verificare che il personale esegua correttamente e nella giusta sequenza le azioni previste dalle procedure di sicurezza nei cantieri.** Es: verificare se il lavoratore indossa i dispositivi di protezione (caschi, occhiali, guanti) oppure sono state effettuate le operazioni di lavaggio e disinfestazione delle tute e attrezzature al fine di decontaminarle da sostanze nocive per la salute umana. ***Qui oltre al riconoscimento immagini si realizza l'ulteriore funzione mediante specifici software di analisi dei movimenti dei lavoratori.***



# Come funziona la *computer vision*

Per capire come una macchina possa riconoscere gli oggetti all'interno di immagini e riprese video, conviene partire dalla una definizione scientifica di intelligenza artificiale: l'insieme di sistemi hardware e software che mirano a replicare alcune capacità tipiche dell'essere umano, come la capacità di percepire l'ambiente e interagire con esso.

L'IA, inoltre, è in grado di perseguire in modo autonomo un obiettivo definito, prendendo decisioni per supportare (o sostituire) l'intervento umano.

Così i sistemi di *Computer Vision* sfruttano i sensori ottici di videocamere, fotocamere e altri dispositivi per effettuare riconoscimenti di persone e oggetti; ***alla base della visione artificiale c'è la progettazione di reti neurali stratificate che permettono alla Computer Vision di sviluppare processi di apprendimento caratteristici del cervello umano.***



# La capacità di rilevare situazioni di pericolo per lavoratori e macchinari

- ✓ Rilevare situazioni di potenziale pericolo per coloro che operano nelle aree di lavoro (es: transito di mezzi pesanti e la presenza di carichi sospesi).
- ✓ Il sistema di IA è in grado di: (i) ***inviare tempestivamente*** ed automaticamente segnali di allarme sui dispositivi mobili del personale che opera nell'area di lavoro; (ii) ***registrare*** video e foto da trasmettere in tempo reale su piattaforme IoT.



# Grazie per l'attenzione



Relatore : avv. Roberto Scavizzi

Commissione 231 seminario 6 Novembre 2025

Data