REGOLAMENTO EUROPEO SULL'INTELLIGENZA ARTIFICIALE

2024/1689

AI COMPLIANCE:
QUELLO CHE LE AZIENDE DEVONO SAPERE PRIMA DI USARE L'INTELLIGENZA ARTIFICIALE

AVVERA | SB Società Benefit

AGENDA

AVVERA | SB Società Benefit

- I principi alla base e gli obbiettivi del Regolamento;
- Fasi di attuazione e termini da rispettare;
- Ruoli, obblighi e responsabilità;
- Classificazione dei rischi e conseguenze pratiche;
- Come mitigare il rischio per evitare le sanzioni;
- Approcci per una gestione agile ed efficace.

PERCHÉ SI PARLA DI AI?

AVVERA

L’intelligenza artificiale è divenuta un **fenomeno sociale di portata globale,** soprattutto grazie alla diffusione dei sistemi di AI generativa.

Il lancio di ChatGPT a fine 2022 ha innescato un processo di «democratizzazione» dell’AI.

L'AI IN AZIENDA

- Nel 2024 il mercato nazionale dell'AI ha toccato 1,2 miliardi di euro, in aumento del + 58% rispetto all'anno precedente. Si stima che l'AI potrebbe contribuire per oltre il 15% del PIL entro il 2030.

- L'AI sta cambiando il modo di lavorare dei **colletti bianchi**, ma non i valori e i doveri fondamentali: il compito è governare il cambiamento tecnologico preservando tali valori.

- Secondo lo studio "AI Radar" pubblicato da Boston Consulting Group (BCG) in occasione del World Economic Forum di Davos, è emerso che l'Italia tra i paesi più arretrati per formazione dei dipendenti in materia di AI/Generative AI, con solo il 20% delle aziende che ha formato almeno un quarto dei dipendenti.

L’AI IN AZIENDA

Il percorso iniziato dodici anni fa partiva da una domanda semplice: come aiutare i dipendenti a raggiungere l’inventario più facilmente? Oggi la risposta è un ecosistema complesso in cui AI, robotica e capitale umano coesistono per costruire il futuro della logistica intelligente.

https://www.ai4business.it/intelligenza-artificiale/amazon-raggiunge-un-milione-di-robot-e-lancia-deepfleet-il-nuovo-modello-della-logistica/?utm_campaign=ai4business_nl_20250703&utm_source=ai4business_nl_20250703&utm_medium=email&sfdcid=003Tk00000HyDGjIAN>

TECNOLOGIA

Amazon raggiunge un milione di robot e lancia DeepFleet, il nuovo modello della logistica

Home > Intelligenza Artificiale

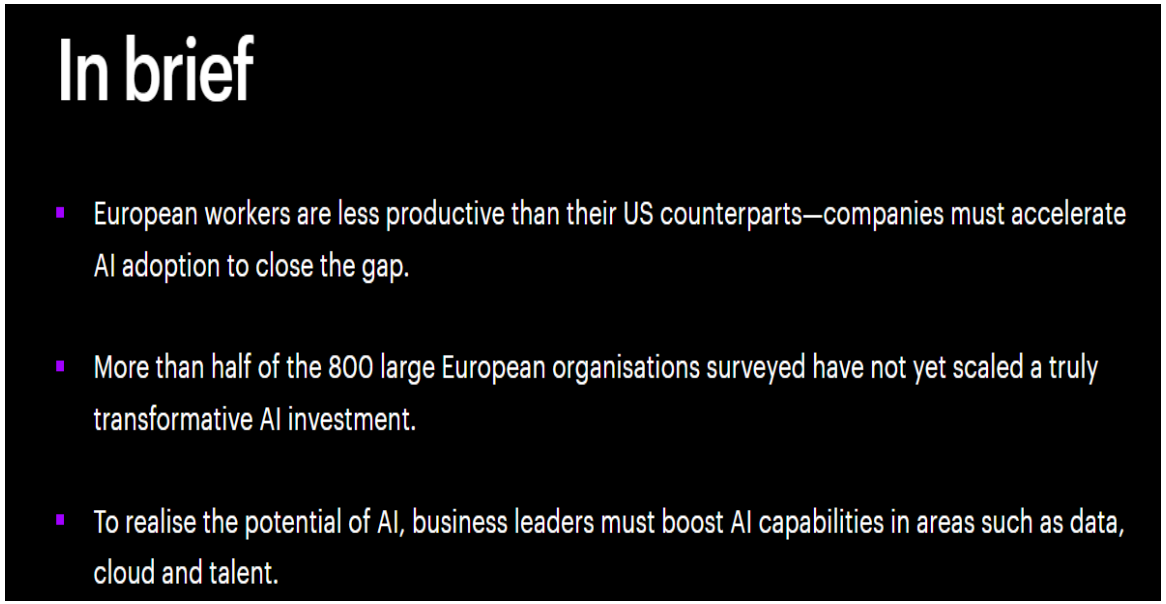
Presentato un modello fondazionale di intelligenza artificiale generativa progettato per migliorare del 10% l’efficienza dei robot. La nuova tecnologia ottimizza i percorsi, accelera le consegne e riduce i costi, con benefici tangibili per clienti, dipendenti e sostenibilità. Circa il 75% delle consegne globali di Amazon è assistito in qualche modo dalla robotica

Pubblicato il 1 lug 2025

L'AI IN AZIENDA:EUROPA

AVVERA

Oggi, in media, un lavoratore europeo produce solo il 76% di quanto produce il suo omologo americano, un dato significativo se si considera che nel 1996 erano alla pari. La causa principale di questo divario è chiaramente la persistente sotto-investimento in tecnologia, una tendenza già esplorata da Accenture nel suo rapporto "Innovate or Fade".



https://www.accenture.com/gb-en/insights/data-ai/europes-ai-reckoning

generated by human

REGOLAMENTO (UE)
2024/1689

- Il 1° agosto è entrato ufficialmente in vigore il Regolamento sull' AI dell'UE (AI Act), con l'obbiettivo di promuovere uno sviluppo e un'implementazione responsabile dell'AI in tutta l'Europa.

- Un atto normativo caratterizzato dall'introduzione di un approccio basato sul rischio, classificando le applicazioni dell'AI in base al loro impatto sui diritti fondamentali.

- Il regolamento dell'UE sull'intelligenza artificiale è il primo atto legislativo al mondo a disciplinare la materia: definisce e armonizza i principi applicabili alla diffusione delle tecnologie basate su intelligenza artificiale, allineandosi ai valori e ai diritti fondamentali cardine della visione europea.

GLI SCOPI DEL REGOLAMENTO

AVVERA

- **migliorare il funzionamento del mercato interno**, istituendo un quadro giuridico uniforme per quanto riguarda lo sviluppo, l'immissione sul mercato, la messa in servizio e l'uso di sistemi di intelligenza artificiale nell'Unione, in conformità dei valori dell'Unione;
- promuovere la diffusione di un'intelligenza artificiale (IA) **antropocentrica** e **affidabile**;
- garantire un livello elevato di protezione della salute, **della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea,** compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente;
- proteggere contro gli **effetti nocivi** dei sistemi di IA nell'Unione (enormi potenzialità trasformative dell'AI, ma non è esente da rischi: bias dei dati, opacità delle decisioni, allucinazioni);
- **Promuovere l'innovazione** (es. Sandbox).

AMBITO DI APPLICAZIONE

DEFINIZIONI (Art. 3 AI Act)

- «**Sistema di intelligenza artificiale**»: "**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".

- «**Modello di AI per finalità generali**»: "addestrato con grandi quantità di dati utilizzando l'autosupervisione su larga scala, che sia caratterizzato una generalità significativa e sia in grado di svolgere con competenza un'ampia gamma di compiti distinti, indipendentemente dalle modalità con cui il modello è immesso sul mercato, e che può essere integrato in una varietà di sistemi o applicazioni a valle".

AMBITO DI APPLICAZIONE

AVVERA

Buona parte del Regolamento è indirizzato ad aziende ("**Provider**") che sviluppano e forniscono sistemi AI; tuttavia, i requisiti principali si applicano a chiunque utilizzi ("**Deployer**") sistemi AI, in quanto, in molte situazioni, **è lo scopo dell'utilizzo che ne determina i possibili impatti e rischi:**

- **Fornitore:** una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che **sviluppa** un sistema di IA o un modello di IA per finalità generali **o che fa sviluppare** un sistema di IA o un modello di IA per finalità generali **e immette tale sistema o modello sul mercato o mette in servizio il sistema di IA con il proprio nome o marchio**, a titolo oneroso o gratuito.

- **Deployer:** la persona fisica o giuridica, autorità pubblica, agenzia o altri organismi **che utilizzano un sistema di IA sotto la propria autorità**, ad **eccezione** nel caso in cui il sistema di IA sia utilizzato nel corso di **un'attività personale non professionale**.

2

AVVERA | SB Società Benefit

FASI DI ATTUAZIONE E TERMINI DA RISPETTARE

AVVERA SRL SB

FASI DI ATTUAZIONE

Data di entrata in vigore dell' AI Act	**01/08/2024**
Data di applicazione delle disposizioni dell' AI Act , salve le eccezioni previste per le specifiche disposizioni	**02/08/2026**
Data di applicazione obbligo di alfabetizzazione art. 4 e dei divieti di cui all'art. 5	**02/02/2025**
Data di applicazione delle disposizioni relative ai modelli di GPAI	**02/08/2025**
Data di applicazione delle disposizioni relative ai sistemi di IA ad alto rischio elencati nell' Allegato III	**02/08/2026**
Data di applicazione delle disposizioni relative ai sistemi di IA ad alto rischio, di cui all'articolo 6, par. 1	**02/08/2027**

GPAI: IL CODICE DI CONDOTTA

Scopo:
Il Codice di Condotta GPAI è uno strumento volontario che aiuta le aziende fornitrici di modelli di intelligenza artificiale a uso generale a rispettare le disposizioni del Regolamento europeo sull'AI (AI Act), soprattutto riguardo a sicurezza, trasparenza e rispetto del diritto d'autore.

Contesto e tempistiche:
- Pubblicato il 10 luglio 2025
- Nei giorni seguenti, la Commissione Europea e gli Stati membri ne valuteranno l'adeguatezza
- Sarà integrato da linee guida ufficiali della Commissione su concetti chiave, previste entro fine luglio


European Commission

The General-Purpose AI Code of Practice

The General-Purpose AI (GPAI) Code of Practice is a voluntary tool, prepared by independent experts (https://digital-strategy.ec.europa.eu/en/news/meet-chairs-leading-development-first-general-purpose-ai-code-practice) in a multi-stakeholder process, designed to help industry comply with the AI Act's obligations for providers of general-purpose AI models. Read more about the timeline of the drafting process of the Code (https://digital-strategy.ec.europa.eu/en/policies/ai-code-practice).

The Code was published on July 10, 2025. In the following weeks, Member States and the Commission will assess its adequacy. Additionally, the code will be complemented by Commission guidelines on key concepts related to general-purpose AI models, to be published still in July.

More information on the code is available in this dedicated Q&A (https://digital-strategy.ec.europa.eu/en/faqs/general-purpose-ai-models-ai-act-questions-answers).

The three chapters of the Code

Below you can download the code, consisting of three separately authored chapters: Transparency, Copyright, and Safety and Security.

https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai

3

AVVERA | SB Società Benefit

RUOLI OBBLIGHI E RESPONSABILITÀ

AVVERA SRL SB

I NUOVI RUOLI IN AZIENDA

AVVERA

AI Compliance Officer: punto di riferimento per tutte le questioni relative alla conformità dei sistemi di intelligenza artificiale utilizzati dall'azienda. La designazione è obbligatoria per i fornitori di sistemi di intelligenza artificiale ad alto rischio

Il Responsabile del sistema di gestione qualità: garanzia che i sistemi di intelligenza artificiale ad alto rischio siano sviluppati, implementati e monitorati secondo standard qualitativi adeguati.

Comitato Etico: obbligatorio per gli enti pubblici e le grandi imprese. Un organo collegiale con composizione multidisciplinare, che dovrà includere giuristi, tecnici e filosofi. Compito di valutare le implicazioni etiche dei sistemi di intelligenza artificiale utilizzati dall'azienda, garantendo **che il loro sviluppo e utilizzo avvenga nel rispetto dei diritti fondamentali e dei valori europei**.

GOVERNANCE E SUPERVISIONE

AVVERA

Per garantire la conformità e un'applicazione efficace delle regole, l' AI Act prevede la creazione di un sistema di governance multilivello, con autorità a livello nazionale e a livello europeo:

In tale contesto in **Italia**, con una legge ora in fase di approvazione finale in Senato (Il Disegno di Legge 1146/24), si attribuiscono le funzioni di vigilanza all'**Agenzia nazionale per la cybersicurezza**, mentre le funzioni di notifica all'**Agenzia per l'Italia digitale.**

OBBLIGO DI ALFABETIZZAZIONE

AVVERA

Livello sufficiente di «alfabetizzazione»:

Al fine di ottemperare all'obbligo preposto dall'Art. 4, sarà necessario sviluppare piani formativi e piani strategici specifici mirati a definire ruoli, processi e responsabilità nell'ottica di una governance dell'IA estesa lungo tutto il ciclo di vita dei sistemi

Le organizzazioni devono prepararsi adeguatamente alla piena applicazione di queste prime disposizioni discusse in questo articolo, dando priorità ad alcune attività:

- Mappare i sistemi di AI utilizzati/sviluppati/forniti per identificare eventuali pratiche proibite.
- Strutturare programmi di formazione conformi ai requisiti di alfabetizzazione sull'AI.
- Implementare sistemi di monitoraggio e documentazione delle attività svolte.
- Mantenersi aggiornati sulle linee guida che verranno pubblicate dalle autorità competenti e prevedere un piano di adeguamento strutturato tenendo conto delle ulteriori previsioni dell'AI Act che diventeranno applicabili nel prossimo futuro

SANZIONI

L'importo delle sanzioni è calcolato sulla base di una percentuale del fatturato complessivo realizzato dalla società nell'anno precedente o su un importo fisso, se superiore. Le PMI e le start-up sono soggette a sanzioni pecuniarie proporzionali.

Struttura su tre livelli:

i. **fino a 35 milioni di euro o al 7% del fatturato mondiale totale annuo dell'esercizio precedente (se superiore)** per violazioni relative a pratiche vietate o per l'inosservanza di requisiti in materia di dati;
ii. **fino a 15 milioni di euro o al 3% del fatturato mondiale totale annuo dell'esercizio precedente** per l'inosservanza di qualsiasi altro requisito o obbligo del regolamento;
iii. **fino a 7,5 milioni di euro o all'1,5% del fatturato mondiale totale annuo dell'esercizio precedente** per la fornitura di informazioni inesatte, incomplete o fuorvianti agli organismi notificati e alle autorità nazionali competenti in risposta a una richiesta.

4

AVVERA | SB Società Benefit

CLASSIFICAZIONE DEI RISCHI E CONSEGUENZE PRATICHE

CHE COS'È L'INTELLIGENZA ARTIFICIALE

AVVERA

L'Intelligenza Artificiale è una disciplina dell'informatica che studia lo sviluppo dei sistemi hardware e software dotati di capacità tipiche dell'essere umano:

- **Apprendimento;**
- **Interazione con l'ambiente;**
- **Adattamento;**
- **Ragionamento e pianificazione.**

FUNZIONAMENTO E RISCHI

AVVERA

I sistemi di Ai si basano su meccanismi di autoapprendimento: «*machine learning*»:

A differenza dei tradizionali algoritmi, costituiti da una serie di regole fisse e predeterminate, il *machine learning* è costituito da regole che variano continuamente in base ad analisi statistiche di grandi quantità di dati. Questi sistemi sono caratterizzati per operare con un notevole tasso di autonomia, che può limitare la trasparenza e favorire l'opacità. ***Black box***

RISCHI E QUALITÀ DEI DATI

Il funzionamento dei sistemi di AI può essere compromesso da:

- Errori di progettazione;
- Difetti dei dati utilizzati nella fase di apprendimento.

- ***Allucinazioni: Garbage in, Garbage out***: con riferimento ai sistemi di AI generativa e la produzioni di che ricorrono in presenza sia di contenuti errati, sia di dati non più attuali o esatti, i quali sono però proposti come risultato di un processo di elaborazione a partire dalle richieste formulate dagli utenti.

- **Bias e discriminazioni:** addestrando gli algoritmi sulla base di dati parziali e potenzialmente affetti da pregiudizi, gli esiti partoriti dall'AI in sede di decision-making riflettono tali bias traducendosi in determinazioni discriminatorie.

RISCHIO INACCETTABILE

AVVERA

L'AI Act vieta che i sistemi considerati come fonte di rischi inaccettabili per la dignità umana e per i diritti fondamentali della persona:

Software che:

- impiegano **tecniche subliminali**;
- sfruttano la vulnerabilità di specifici gruppi per distorcere il comportamento delle persone pregiudicando la loro capacità di prendere una decisione informata in modo che possa derivare un danno significativo;
- permettono forme di ***social scoring*** da cui possa discendere un trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di gruppi di persone;
- effettuino una **valutazione del rischio di commissione di reati** sulla base della profilazione di una persona fisica o della valutazione dei tratti e delle caratteristiche della personalità;
- utilizzano determinate finalità tecniche di riconoscimento facciale o di **categorizzazione o identificazione biometrica** remota in tempo reale in spazi aperti al pubblico.

RISCHIO ALTO

Sistemi di AI che, comportando un alto rischio di violazione dei valori e dei diritti fondamentali, sono assoggettati a una stringente disciplina.

I sistemi che:

- collegati a prodotti che rientrano nell'ambito di applicazione della normativa di armonizzazione dell'UE e per i quali è prevista la verifica di conformità affidata a soggetti terzi;

- alla luce della loro finalità prevista, presentano un alto rischio di pregiudicare la salute e la sicurezza o i diritti fondamentali delle persone e che sono utilizzati nei settori indicati **nell'Allegato III del regolamento.** (ciò comporta che la presunzione di alto rischio è superabile se l'AI non influenza in modo sostanziale la decisione umana).

RISCHIO ALTO

L’allegato III include:

- I sistemi di identificazione o classificazione biometrica;
- Sistemi impiegati per la gestione di infrastrutture critiche;
- **Sistemi impiegati per la selezione o la valutazione di studenti e lavoratori**;
- Sistemi impiegati per l’accesso e la fruizione di prestazione a servizi privati e pubblici essenziali;
- Sistemi impiegati per attività di prevenzione o repressione del crimine;
- Sistemi impiegati per la gestione della migrazione, dell’asilo e del controllo delle frontiere;
- Sistemi impiegati per lo svolgimento dell’attività giurisdizionale.

RISCHIO ALTO

Il regolamento prevede per i sistemi di AI ad alto rischio una serie di obblighi e divieti volti a garantirne la trasparenza, l'affidabilità ed il controllo da parte dell'uomo.

- **Valutazione di conformità e l'apposizione della marcatura CE:** il controllo di conformità è affidato al fornitore del sistema di AI, con l'eccezione dei sistemi destinati a essere utilizzati per la biometria.
- **Registrazione presso la banca dati dell'UE, prima della loro immissione sul mercato;**
- **Gestione dei rischi;**
- **Governance dei dati;**
- **Trasparenza e tracciabilità;**
- **Documentazione tecnica;**
- **Supervisione umana;**
- **Cybersecurity, accuratezza e robustezza.**

RISCHIO LIMITATO

Per i sistemi da cui discende un rischio limitato per i diritti fondamentali, come i chatbot, sono previsti meri obblighi di trasparenza: fornire agli utenti un'informativa per renderli a conoscenza che stanno interagendo con una macchina e non con una persona.

- **Chatbot e assistenti virtuali;**
- **Sistemi di AI che generano o manipolano contenuti audio o video (es. deepfake)**
- **Sistemi di AI utilizzati per la personalizzazione dei contenuti sui social media.**

RISCHIO MINIMO O NULLO

La maggior parte dei sistemi di IA rientra in questa categoria e non è soggetta a obblighi specifici previsti dal Regolamento, ma dovranno comunque rispondere ai requisiti previsti dal Regolamento Generale per la Protezione dei Dati (Regolamento 2016/679/UE), dalla Direttiva Copyright (Direttiva 2019/790/UE), dalla Direttiva sulla responsabilità da prodotto difettoso (adottata in seduta plenaria il 12 marzo 2024, per l'aggiornamento della Direttiva 85/374/CEE) e delle specifiche normative di settore.

- **Filtri spam nelle email;**
- **Sistemi di AI utilizzati nei videogiochi;**
- **Sistemi di raccomandazione per prodotti in un e-commerce (con alcune eccezioni);**
- **Sistemi di AI utilizzati per l'ottimizzazione dei processi industriali.**

MODELLI DI AI PER FINALITÀ GENERALI.

AVVERA

I sistemi GPAI, se non presentano un rischio sistemico, sono sottoposti unicamente ad obblighi di trasparenza e di tutela del copyright.

Scatta una regolamentazione più pervasiva, solo quando emerge un rischio sistemico: prevedendo obblighi ulteriori di sicurezza e protezione
(es. Per esempio **GPT-4 di OpenAI, Gemini di Google, LaMA in casa Meta**)

4

AVVERA | SB Società Benefit

COME MITIGARE IL RISCHIO PER EVITARE SANZIONI

I RISCHI DEGLI USI DELL'AI

AVVERA

Bias algoritmico e discriminazione

L'IA può replicare – o amplificare – pregiudizi contenuti nei dati di addestramento, generando risultati discriminatori nei confronti di dipendenti, clienti o candidati.

Violazioni della normativa sulla privacy (GDPR)

Molti strumenti di IA trattano dati personali. Senza una corretta gestione, si rischiano violazioni gravi del **Regolamento UE 2016/679,** con sanzioni fino a 20 milioni di euro o al 4% del fatturato annuo.

Dipendenza da strumenti AI

Rischi per la salute mentale e il benessere professionale derivato dall'utilizzo dei sistemi di AI.
Uno dei dibattiti aperti tra sociologi e antropologi è se l'utilizzo vada ad impigrirci e a disimparare a svolgere determinate attività. Es. scrivere e-mail professionali o di pensare in maniera critica.

I RISCHI DEGLI USI DELL'AI

AVVERA

Bias Algoritmico e discriminazioni

APPROFONDIMENTO

Cos'è il position bias negli LLM e come mitigarlo

Home > Intelligenza Artificiale

Si tratta di un limite strutturale degli LLM che li porta a privilegiare le informazioni poste all'inizio e alla fine di un testo, trascurando quelle centrali. In ambito aziendale, questo può risultare problematico. Ecco come mitigarne gli effetti con strategie pratiche

Pubblicato il 27 giu 2025

https://www.ai4business.it/intelligenza-artificiale/cose-il-position-bias-negli-llm-e-come-mitigarlo/

generated by human

I RISCHI DEGLI USI DELL'AI

Dipendenza

Futurism

NEW HIRE | JUL 3, 9:29 AM EDT *by* FRANK LANDYMORE

OpenAI Says It's Hired a Forensic Psychiatrist as Its Users Keep Sliding Into Mental Health Crises

"We're developing ways to scientifically measure how ChatGPT's behavior might affect people emotionally."

/ Artificial Intelligence / AI Chatbots / Chatgpt / OpenAI

https://futurism.com/openai-forensic-psychiatrist

I RISCHI DEGLI USI DELL'AI

AVVERA

Responsabilità legale per decisioni automatizzate

Se un sistema IA prende decisioni che incidono sui diritti delle persone (es. selezione del personale, accesso al credito, valutazione delle performance), l'azienda è chiamata a rispondere – anche in assenza di dolo.

Impatti ambientali

Grande quantità di energia e grandi quantità di acqua per far raffreddare i data center in cui i dati vengono localizzati e processati. In particolare la GENAI richiede grande potere computazionale e grandi location per fare lo storage dei dati. Per funzionare bene sono necessarie soluzioni cloud dove i dati vengono localizzati e processati.

Lavoro invisibile e Diritti Umani

dietro ai modelli di GENAI c'è un lavoro umano: questi modelli, prima che vengano rilasciati sul mercato, ci sono migliaia di addestratori che fisicamente vanno a verificare che l'output sia accurato e sulla base di questo danno un feedback. Dietro di loro ci sono migliaia di annotatori di dati.

LE MISURE PER MITIGARE I RISCHI

- **Sfida sul piano della privacy e della sicurezza**: Uso etico dei sistemi di AI, basato sulla tutela dei dati. È essenziale dare priorità a un utilizzo sicuro degli strumenti di AI generativa – proteggere le informazioni sensibili (personali, dei propri clienti e della propria azienda) è di fondamentale importanza (art. 10, 14 AI Act);

- **Misure di supervisione umana e trasparenza :** Gli operatori devono essere in grado di poter comprendere e interpretare l'output del sistema di AI, monitorare e, se necessario, intervenire o disattivare il sistema. Art. 14 AI Act per i sistemi ad alto rischio, garanzia di una sorveglianza umana efficace, capace di intervenire e controllare il sistema per ridurre i rischi associati al suo utilizzo.

- **Formazione e Re-skilling:** strategia necessaria per lo sviluppo di competenze specifiche che possono tradursi in un vantaggio competitivo sostanziale.

BEST PRACTICES

Implementare un sistema di compliance robusto che possa integrare etica, diritto, sicurezza e governance:
La designazione di un responsabile per la conformità all' AI Act;
Sviluppare procedure interne per garantire la conformità continua.

Mappare e classificare:
Mantenere una documentazione completa e aggiornata su tutti gli i tipi di AI e aspetti dei sistemi di AI
Prepararsi a fornire questa documentazione alle autorità se richiesta.

Formazione del personale:
Assicurare che tutto il personale coinvolto nello sviluppo e nell'utilizzo di sistemi di AI sia adeguatamente formato sulle disposizioni dell'AI Act.

BEST PRACTICES

AVVERA

Monitoraggio proattivo:
Implementare sistemi robusti di monitoraggio dopo l'immissione sul mercato;
Sviluppare processi per l'identificazione e la segnalazione tempestiva di incidenti.

Collaborazione con le autorità:
Adottare un approccio collaborativo con le autorità di vigilanza
Considerare la partecipazione a consultazioni pubbliche e iniziative di settore.

Prepararsi alle ispezioni:
Sviluppare protocolli interni per gestire eventuali ispezioni o richieste di informazione da parte delle autorità.

Gestione del rischio:
Incorporare considerazioni relative all'AI Act nella strategia complessiva di gestione del rischio aziendale.

6

AVVERA | SB Società Benefit

APPROCCI PER UNA GESTIONE AGILE ED EFFICACE

AVVERA SRL SB

ROADMAP DI ADEGUAMENTO

AVVERA

I passi da compiere:

- **Implementazione: -** entro febbraio 2025 - dotarsi **di policy relative alle pratiche vietate dall'articolo 5 del Regolamento.**
- **Se utilizzo GPAI**: - entro il 2 agosto 2025 - Garantire la trasparenza obbligatoria (informative), implementare una policy di compliance sul diritto d'autore, adottare misure di sicurezza per modelli ad alto rischio sistemico.
- **Certificazione**: - entro agosto 2026

COME INTEGRARE L' AI?

AVVERA

📄 Documento di Gap Analysis iniziale

- Obiettivo: mappatura dei sistemi IA presenti in azienda.
- Contenuti:
  - Classificazione dei sistemi AI (vietati, ad alto rischio, generici, ecc.)
  - Ruolo dell'organizzazione rispetto ai sistemi (provider, deployer, user, ecc.)
  - Verifica della presenza di dataset usati per l'addestramento
  - Analisi dell'impatto su diritti fondamentali e discriminazione

⚖️ Documento di Classificazione del Rischio

- Classificazione dei sistemi IA secondo l'AI Act:
  - Vietati (Art. 5)
  - Alto rischio (Titolo III, Capo 1)
  - Generici/General Purpose (Titolo III, Capo 5)
  - Basso rischio
- Strumenti: griglia decisionale + scheda per ciascun sistema

📘 Politica Aziendale sull'IA

- Documento di governance interna.
- Contenuti:
  - Principi etici
  - Ruoli e responsabilità
  - Modalità di classificazione e monitoraggio
  - Obblighi di trasparenza
  - Procedure per l'adozione di nuovi sistemi IA

COME INTEGRARE L' AI?

AVVERA

Modello di Contratto/Clausole Contrattuali sull'IA

- Per fornitori o acquirenti di sistemi IA.
- Include:
  - Clausole di conformità all'AI Act
  - Requisiti documentali
  - Garanzie sull'uso dei dataset
  - Audit, monitoraggio e notifiche

Informative di Trasparenza per gli Utenti Finali

- Obbligatorio per alcuni sistemi (es. chatbot, deepfake, recommendation system).
- Include:
  - Avvertenza che si interagisce con IA
  - Finalità
  - Diritto a ottenere intervento umano (se previsto)

Procedura di Notifica alle Autorità

- Template per la notifica dei gravi incidenti o violazioni.
- Include:
  - Tracciato informativo standard
  - Destinatari

Framework di Audit Interno

- Checklist di controllo periodico.
- Include:
  - Verifica dei requisiti tecnici
  - Monitoraggio delle performance
  - Conformità ai registri obbligatori
  - Aggiornamento della documentazione

NUOVE DINAMICHE DEL LAVORO

AVVERA

L'implementazione dei sistemi di AI in azienda, se utilizzati in modo consapevole, garantiscono un vantaggio competitivo:

- Nuove opportunità di innovazione;
- Riduzione tempi di produzione;
- Accelerazione tempi di sviluppo;
- Apertura di nuove possibilità per prodotti, servizi ed esperienze;
- Efficienza e qualità del lavoro in team: supporto tecnologico che facilita e arricchisce le fasi del progetto;
- Maggiore produttività e stimolo della creatività (chiedere nuove idee, vedere un problema da prospettive diverse, simulazione di scenari).

Report finale della consultazione

Linee guida per l'implementazione dell'intelligenza artificiale nel mondo del lavoro

Strumenti pratici e raccomandazioni per un uso responsabile, sicuro e antropocentrico dell'IA nel mondo del lavoro

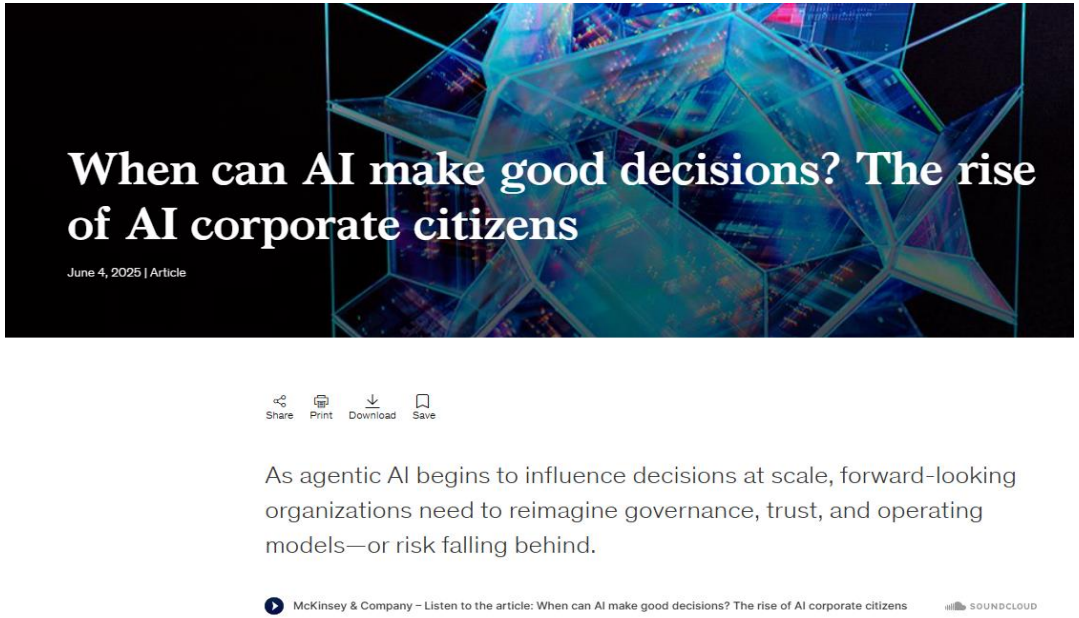
https://www.lavoro.gov.it/stampa-e-media/multimedia/report-finale-della-consultazione

generated by human

AI AGENTICA

L’agentic AI non si limita a eseguire compiti predefiniti, ma agisce autonomamente, ragionando, adattandosi e collaborando con altri agenti AI per ottimizzare processi complessi come l’analisi del credito, la gestione del rischio e la conformità normativa:

- **Ripensare alla governance**: una governance trasparente per evitare rischi di bias e responsabilità sfocate;
- **Fiducia e modelli operativi**: nuove forme di collaborazione tra l’AI automatizza sui compiti ripetitivi mentre gli umani si concentrano su supervisione, giudizio e decisioni complesse. Per questo servono investimenti in infrastrutture dati moderne, formazione del personale e cambiamenti culturali per integrare efficacemente l’AI nella strategia aziendale.



https://www.mckinsey.com/capabilities/operations/our-insights/when-can-ai-make-good-decisions-the-rise-of-ai-corporate-citizens#/

REGOLAMENTO EUROPEO SULL'INTELLIGENZA ARTIFICIALE

2024/1689

AI COMPLIANCE:
QUELLO CHE LE AZIENDE DEVONO SAPERE PRIMA DI USARE L'INTELLIGENZA ARTIFICIALE

AVVERA | SB Società Benefit