

Bonn, Bucharest, Dublin, Lisbon, Madrid, Milan, Paris, The Hague, Vienna, Warsaw

Come definire un sistema di Intelligenza Artificiale ai sensi dell'AI Act

CEDPO AI and Data Working Group

Micro-Insights Series

Ottobre 2025

Authors:

Marc Bellon

Lionel Capel

Maria Moloney

Laura Morató Pascual

Alessandro Vasta

Contatti:

<https://cedpo.eu>

info@cedpo.eu

Informazioni sulla serie Micro-Insights

La serie *Micro-Insights* è un'iniziativa editoriale del gruppo CEDPO AI and Data Working. Essa fornirà dei documenti leggeri di facile comprensione, definitivi e sintetici su temi di interesse relativi all'intersezione tra i dati e l'intelligenza artificiale.

Con un approccio pratico, volto a spiegare sia argomenti complessi sia a darne implementazione, la serie illustrerà l'importanza delle aree chiave e fornirà consigli ai professionisti sull'impatto e sui passi successivi. Con l'entrata in vigore della legge dell'UE sull'Intelligenza Artificiale (la "legge sull'AI") avvenuta nel 2024, la scena è ora pronta per tutti i professionisti ed è possibile discutere la regolamentazione dei dati e dell'AI con molta maggiore chiarezza.

La serie *Micro-Insights* seguirà l'evoluzione dell'AI e dei dati nei prossimi anni e alla luce dell'avvicinarsi della scadenza del periodo cruciale per l'attuazione dell'AI Act nonché dell'evoluzione sempre più innovativa e inaspettata delle tecnologie di AI, la serie fornirà una guida aggiornata e autorevole sulle principali aree di interesse.

Tra gli altri, la serie includerà documenti su:

- Regolamentazione ai sensi dell'AI Act dell'Intelligenza Artificiale per scopi generali
- Spiegazione del AI Pact.
- Formazione dei professionisti su come condurre valutazioni d'impatto sui diritti fondamentali (Fundamental Rights Impact Assessments - FRIA) ai sensi dell'AI Act.
- Delineazione del ruolo che le autorità di regolamentazione della protezione dei dati avranno nella regolamentazione dell'AI.
- Esame dell'idoneità o non del responsabile della protezione dei dati (RPD/DPO) a ricoprire il ruolo the AI Officer.
- Basi giuridiche per l'utilizzo dei dati di addestramento.
- Un kit di strumenti per la preparazione all' AI Act

INDICE

1.	Introduzione	4
2.	Criteri dei Sistemi AI	5
	Sistema automatizzato	5
	Livelli variabili di autonomia	5
	Adattabilità dopo la diffusione	6
	Obiettivi	6
	Inferenza	6
	Outputs	7
	Influenza sugli ambienti	7
3.	Conclusione	7

1. Introduzione

Uno dei principali obiettivi dell'AI Act è di favorire l'innovazione nell'ambito dell'AI garantendo al contempo elevati livelli di tutela della salute, della sicurezza e dei diritti fondamentali all'interno dell'Unione europea. È essenziale comprendere l'ambito di applicazione del regolamento per poter individuare con precisione ciò che rientra nel suo campo e ciò che non rientra. Solo i sistemi che soddisfano la definizione di *sistema di intelligenza artificiale* contenuta nel regolamento ricadono nel suo ambito di applicazione.

Data la complessità della normativa, alla Commissione europea è richiesto di fornire delle linee guida volte ad aiutare i soggetti interessati a comprendere e applicare la definizione di sistema di AI perimetrata dall'AI Act.

A tale scopo, il 6 febbraio 2025 la Commissione ha pubblicato delle *guidelines* per aiutare gli interessati a comprendere meglio la definizione di sistemi di AI indicata nell'AI Act e per supportare la fase iniziale di attuazione delle sue disposizioni, entrate in vigore nello stesso mese.

Le linee guida costituiscono un aiuto, ma non sono giuridicamente vincolanti. La competenza per le interpretazioni definitive dell'AI Act spetta alla Corte di giustizia dell'Unione europea (CGUE). Considerata la rapida evoluzione delle tecnologie di intelligenza artificiale, le linee guida sottolineano l'importanza di un'applicazione flessibile e non meccanica della definizione di sistema di AI.

L'articolo 3, paragrafo 1, dell'AI Act definisce un **sistema di intelligenza artificiale** come un sistema basato **su macchine**, dotato di diversi **livelli di autonomia** e potenzialmente in grado di presentare **capacità di adattabilità** dopo la diffusione e che inferisce risultati (previsioni, contenuti, raccomandazioni, decisioni) a partire da **input con l'obiettivo di influenzare ambienti fisici o virtuali**.

Se analizziamo questa definizione, possiamo vedere che ci sono sette criteri principali per i sistemi di AI:

1. Deve essere un sistema automatizzato.
2. Ci devono essere vari livelli di autonomia.
3. Potrebbe presentare adattabilità dopo la diffusione.
4. Devono esserci (almeno uno o più) obiettivi.
5. Deve esserci il processo di inferenza.
6. Devono esserci (uno o più) output.
7. Deve avere un'influenza sul proprio ambiente.

Il resto di questo articolo fornisce spiegazioni molto brevi di ciascuno di questi sette criteri per aiutare il lettore a comprendere in modo pratico la natura di un sistema di AI come definito dall'AI Act.

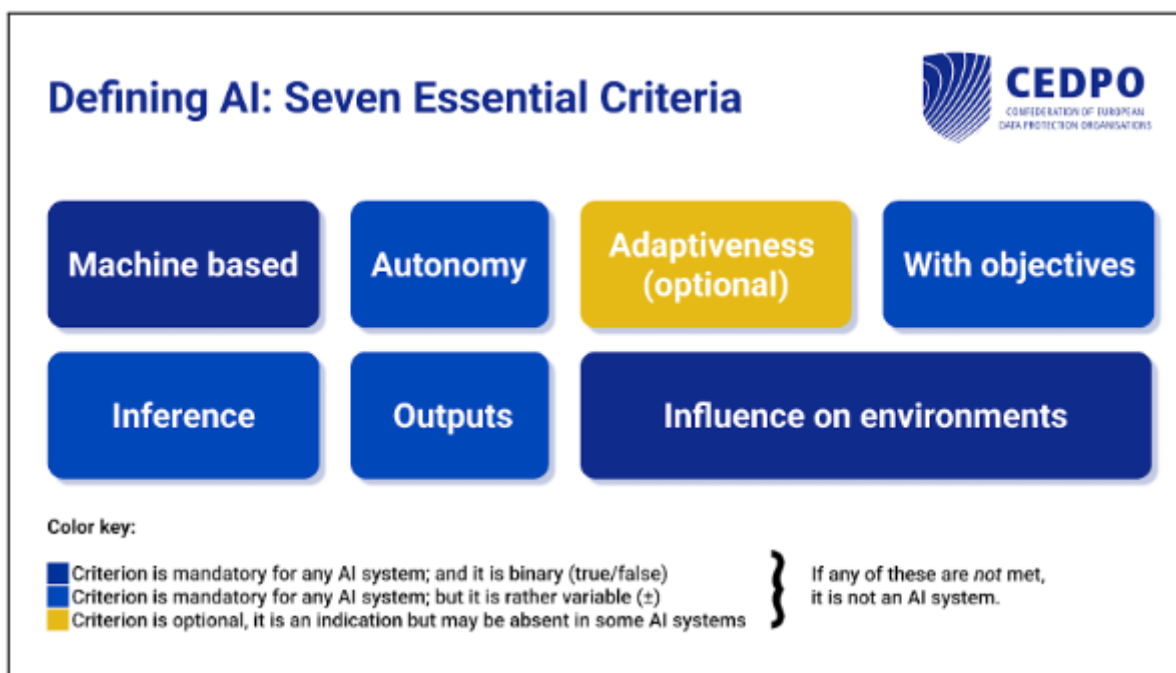


Figure 1 The Seven Criteria for AI Systems

2. Criteri dei Sistemi AI

Sistema automatizzato

Tutti i sistemi di intelligenza artificiale sono sviluppati e funzionano su macchine: hardware (componenti fisici) e software (codice informatico, istruzioni, programmi, sistemi operativi e applicazioni). I sistemi di AI possono basarsi su una pluralità di tali componenti.

Il concetto di “automatizzato” è inteso in senso ampio e comprende anche i sistemi emergenti che si discostano dal calcolo tradizionale, tra cui:

- i sistemi di calcolo quantistico (*quantum computing systems*); e
- i sistemi di calcolo biologico o organico (*biological computing*).

Livelli variabili di autonomia

Per determinare se un sistema possa qualificarsi come sistema di intelligenza artificiale, il livello di autonomia rappresenta un fattore cruciale. I sistemi progettati per operare con un grado ragionevole di indipendenza nelle loro azioni soddisfano il criterio di autonomia previsto nella definizione di sistema di AI.

Un aspetto chiave dell'autonomia riguarda il livello o grado di intervento e coinvolgimento umano. Ad esempio, un sistema come ChatGPT, che necessita di input forniti manualmente per generare un output in modo indipendente, dimostra “un certo grado di indipendenza d'azione”, poiché è in grado di produrre un risultato che sia specificato con precisione da un essere umano.

Adattabilità dopo la diffusione

Un sistema di AI “può mostrare adattabilità dopo la diffusione”. Ciò si riferisce alle capacità di autoapprendimento, ovvero il sistema può apprendere automaticamente, scoprire nuovi patterns o identificare relazioni nei dati che vanno oltre ciò su cui è stato inizialmente addestrato. Ciò consente al sistema di modificare il proprio comportamento durante l'uso, producendo potenzialmente risultati diversi per gli stessi input.

A differenza di altri criteri, tutti essenziali per definire un sistema di AI, l'adattabilità dopo la diffusione non è un criterio decisivo, ma piuttosto un indicatore. Pertanto, un sistema che è stato inizialmente addestrato e che non mostra adattabilità una volta diffuso non è escluso dalla definizione di sistema di AI.

Obiettivi

Gli “obiettivi” di un sistema di AI fanno riferimento ai suoi obiettivi interni, che ne determinano come il sistema funziona. Tali obiettivi possono essere definiti esplicitamente mediante funzioni di ottimizzazione o derivati implicitamente da schemi appresi attraverso l'interazione con l'ambiente circostante. Questi obiettivi possono differire dallo “scopo previsto” assegnato dal provider (fornitore) in un contesto specifico, in quanto si concentrano sugli esiti che il sistema deve raggiungere, senza necessariamente implicare come venga integrato o utilizzato. Di conseguenza, l'AI può sviluppare obiettivi non formulati esplicitamente, come nel caso dei *reinforcement learning models* (modelli di apprendimento per rinforzo) o nei *large language models* (grandi modelli linguistici). Sebbene questa caratteristica sia essenziale per descrivere un sistema di AI, non è sufficiente di per sé per distinguerlo da altri algoritmi

Inferenza

In ambito di AI, il termine “inferenza” si riferisce alla capacità di un sistema di generare output, quali previsioni, contenuti, raccomandazioni o decisioni, sulla base degli input ricevuti. Questo processo comporta la derivazione di conclusioni dai dati, spesso utilizzando tecniche di AI quali il *machine learning* (apprendimento automatico) o approcci basati sulla conoscenza. Nel contesto dell'AI, l'inferenza comprende sia la generazione di risultati dagli input (durante la fase di utilizzo del sistema) sia la derivazione di modelli o algoritmi dai dati durante la fase di sviluppo. Questa capacità di inferire distingue i sistemi di AI dal software tradizionale, che si basa su regole predefinite e non genera output basati su modelli appresi o derivati.

Outputs

La capacità di un sistema di generare output (quali previsioni, contenuti e raccomandazioni) in grado di influenzare ambienti fisici o virtuali, sulla base degli input ricevuti e utilizzando il *machine learning*, la logica e gli approcci basati sulla conoscenza, è fondamentale per il funzionamento dei sistemi di AI e per distinguerli da altre forme di software.

Questi output rientrano in quattro categorie principali: **previsioni, contenuti, raccomandazioni e decisioni**.

Le **previsioni** comportano la stima di valori sconosciuti con un intervento umano minimo. I **contenuti** si riferiscono alla creazione di nuovo materiale come testi e immagini. Le **raccomandazioni** suggeriscono azioni o prodotti sulla base dei dati degli utenti. Le **decisioni** sono conclusioni prese dal sistema che, di fatto, automatizzano il giudizio umano. I sistemi di AI, in particolare quelli che utilizzano *machine learning*, possono eccellere nella gestione di dati complessi e nella generazione di output più sfumati rispetto ai sistemi non basati sull'AI.

Influenza sugli ambienti

Un elemento rilevante nella definizione di un sistema di AI è la sua capacità di produrre output che possono influenzare sia ambienti fisici che virtuali. Ciò evidenzia che i sistemi di AI agiscono come agenti attivi, che influenzano gli ambienti in cui operano.

L'espressione "ambienti fisici o virtuali" comprende sia oggetti tangibili e fisici (come un braccio robotico) che ambienti virtuali, inclusi spazi digitali, flussi di dati e ecosistemi software. Un esempio di sistema AI che influenza un ambiente fisico è un agente che prenota biglietti aerei.

3. Conclusione

L'AI Act dell'Unione Europea fornisce una definizione completa dei sistemi di intelligenza artificiale, articolata in sette criteri chiave come illustrati in questo articolo. Il punto chiave che emerge dalla definizione dei sistemi di AI secondo l'AI ACT è che questi sistemi consistono essenzialmente in codici di software sviluppati utilizzando tecniche come il *machine learning*, metodi statistici e/o altri approcci basati sulla logica, che portano a decisioni, previsioni o raccomandazioni che hanno il potenziale di influenzare i nostri ambienti fisici e virtuali.

Questa definizione complessa cerca di cogliere la natura dinamica e in continua evoluzione dell'AI, cercando al contempo di stabilire basi giuridiche chiare per la sua supervisione. Ancorando i sistemi di AI a questo quadro normativo, l'UE intende stabilire un equilibrio tra la promozione dell'innovazione e la salvaguardia della salute, della sicurezza e dei diritti fondamentali. Ciò a sua volta promuoverà la trasparenza, la responsabilità e la fiducia nello sviluppo e nella diffusione in futuro delle tecnologie di AI in tutta l'Unione.