EU Artificial Intelligence Act

Avv. Paolo Bernardini

REGOLAMENTO (UE) 2024/1689 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 13 giugno 2024 (c.d. AI Act)

01

PUBBLICATO IL

12 LUGLIO 2024

SULLA GAZZETTA UFFICIALE DELL'UNIONE EUROPEA

02

ENTRATO IN VIGORE IL

01 AGOSTO 2024

03

SI **APPLICHERA'** DAL

02 AGOSTO 2025

CON DISPOSIZIONI ANTICIPATE E ALTRE

POSTICIPATE

ROAD MAP DELL'AI ACT

- -I **DIVIETI IA INACCETTABILE** E LE **DEFINIZIONI** E **LE DISPOSIZIONI RELATIVE ALL'ALFABETIZZAZIONE** IN MATERIA DI AI (I CAPI 1 E 2) I **APPLICANO A DECORRERE DAL 2 FEBBRAIO 2025** – 6 MESI DOPO L'ENTRATA IN VIGORE
- LE **NORME SULLA GOVERNANCE** E GLI **OBBLIGHI PER L'IA DI USO GENERALE** (IL CAPO 3, SEZ. 4, IL CAPO 5, 7, 12 E L'ART. 78) **SI APPLICANO A DECORRERE DAL 2 AGOSTO 2025** (AD ECCEZIONE DELL'ART. 101) - 12 MESI DOPO L'ENTRATA IN VIGORE;
- GLI **OBBLIGHI** PER I **SISTEMI DI AI AD ALTO RISCHIO** (L'ART. 6 PARAGRAFO 1 E I CORRISPONDENTI OBBLIGHI DI CUI AL PRESENTE REGOLAMENTO) **SI APPLICANO A DECORRERE DAL 2 AGOSTO 2027** - 36 MESI DOPO L'ENTRATA IN VIGORE;

INTRODUZIONE

In questo incontro avente per tema **IL REGOLAMENTO UE SULL'INTELLIGENZA ARTIFICIALE**, esploreremo
lo **scenario attuale** dell'**Intelligenza Artificiale**,
gli **obiettivi principali** **dell'AI Act**
e la **materia** che viene **disciplinata** al suo interno.

INTRODUZIONE

Concetti decisivi: Intelligenza Artificiale **e** Sistema di IA

Partiamo dalle basi. Cosa si intente per **Intelligenza Artificiale?** Secondo quanto definito dalla **Commissione Europea** nel **2018** e ribadito da più fonti, si definiscono Intelligenza Artificiale i

"Sistemi che mostrano un comportamento intelligente analizzando il loro ambiente e agendo - con un certo grado di autonomia - per raggiungere obiettivi specifici."

INTRODUZIONE

Troviamo anche altre definizioni più semplici, ma che ci aiutano a capire meglio cos'è l'IA.
Il **Parlamento Europeo** l'ha anche definita come
"**l'abilità di una macchina di mostrare capacità umane quali il ragionamento, l'apprendimento, la pianificazione e la creatività**" .
Semplificando quanto detto sopra, possiamo dire che si parla di **macchine** in riferimento ad esempio a device **IoT** (SMARTPHONE, FRIGORIFERI INTELLIGENTI, ALLARMI ANTINCENDIO, ETC.)o **veicoli autonomi** o di **software** capaci di "***pensare***" **in autonomia.**
Tuttavia, il **Regolamento non parla di IA**, ma di **sistemi di IA**. Allora, la domanda che sorge spontanea è:
qual è la differenza tra questi due concetti?

INTRODUZIONE

qual è la differenza tra questi due concetti?

L'Intelligenza Artificiale è un concetto generale che si riferisce alla capacità di una macchina di imitare funzioni cognitive tipiche degli esseri umani

I Sistemi di IA sono applicazioni concrete basate su tecnologie di intelligenza artificiale. Si tratta di applicazioni pratiche dell'IA progettate per svolgere compiti specifici

La **definizione** di **sistema di IA** fornita dal **Regolamento** si approssima alla definizione di IA data dalla Commissione.

INTRODUZIONE

Infatti, il **Regolamento definisce** questi **sistemi** come:

“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” (Art. 2 comma.1 del Regolamento).”

INTRODUZIONE

Inferenza e autonomia

La caratteristica principale e fondamentale di **questi sistemi** è **l'inferenza** **intesa come la capacità di processare le informazioni precedentemente ottenute ed usate per estrarre conclusioni o fare predizioni applicabili a situazioni reali.**

L'inferenza (attraverso gli **algoritmi**, sequenza di istruzioni) comporta il **processo successivo** alla **fase di apprendimento o training** di un **sistema** o **modello di IA** poiché **permette l'IA** di **agire**, in altre parole, ne permette di **proporre soluzioni utili** attraverso l'utilizzo di **strategie** di **apprendimento automatico** (**machine learning**) e di **strategie** che hanno come **base** la **logica** e il **sapere**

Senza inferenza, l'IA non sarebbe in grado di generare soluzioni utili ad affrontare situazioni reali; l'IA non funzionerebbe. Si pensi, ad **esempio**, al sistema di sicurezza della posta elettronica: attraverso l'IA è possibile creare un sistema che, grazie a una strategia di apprendimento automatico, riconosca nel flusso di dati i messaggi di spam o gli attacchi via e-mail (come il pishing, il malware, ecc.) e, attraverso l'inferenza, blocchi automaticamente le e-mail dannose in arrivo. **Senza l'inferenza**, il sistema di sicurezza delle e-mail **non è in grado di fare questo ragionamento logico** e quindi le e-mail non sono protette dallo spam o dagli attacchi via e-mail.

INTRODUZIONE

La **seconda caratteristica** del **sistema di IA** è **l'autonomia**. Come emana dal proprio concetto, i **sistemi di AI** possono essere progettati per funzionare con **livelli di autonomia variabili** ma, anche, possono essere **utilizzati** come **elementi indipendenti (stand-alone)** o come **componenti di un prodotto**. Infatti, **l'autonomia** dei **sistemi di IA** comporta profondi dibattiti sull'impatto che possa avere **sull'essere umano**. Questo argomento ha spinto all'UE a mettere in modo questo nuovo regolamento, in ricerca di un'**IA etica**, **affidabile** **e** **accurata**.

L'essere umano come centro neuralgico

Collegato con quanto appena accennato e come disposto nel ***considerando 6*** del testo normativo, il **legislatore europeo** riconosce **l'Essere Umano** come **centro dell'IA.**

L'IA deve quindi essere una **tecnologia PER le persone** ed avere come **scopo** **l'aumento del loro benessere**.

INTRODUZIONE

Introduzione al mondo dell'Intelligenza Artificiale: l'ambito di applicazione

Il **Regolamento** si focalizza nel **disciplinare** sia i **sistemi IA** come i **prodotti** che come **servizi** a essi connessi.
Deve quindi essere **applicabile** a **tutti i settori**, senza pregiudizio delle norme giuridiche in vigore **nell'Unione Europea** e in **ognuno degli Stati Membri**, e completa il quadro normativo esistente in materia di **protezione di dati personali**, **protezione di minorenni** e di **consumatori**; **diritti fondamentali**; **protezione ai lavoratori, lavoro** e **sicurezza dei prodotti, ecc.**

Tuttavia, **non rientrano nell'ambito di applicazione del Regolamento:**

- i **settori** che non fanno parte del diritto dell'Unione Europea;??
- i **sistemi di IA che**, e nella misura in cui, sono immessi sul mercato, messi in servizio o utilizzati, per **scopi militari**, di **difesa** o di **sicurezza nazionale**, indipendentemente dal tipo di entità che svolge tali attività;
- i **sistemi di IA** sviluppati e messi in servizio per la **sola ricerca e sviluppo scientifico**;

INTRODUZIONE

Introduzione al mondo dell'Intelligenza Artificiale: i soggetti coinvolti

Per capire quali sono i **soggetti** che **devono rispettare** il **Regolamento**, occorre prendere in considerazione tre parole chiave: **sviluppo**, **distribuzione** **e** **utilizzo**.
Sulla base di questi tre termini, è possibile individuare i seguenti operatori:

1. **Qualsiasi persona, fisica o giuridica, o ente pubblico o privato**, che **sviluppi** un **sistema di IA** e/o lo **immetta** sul **mercato europeo** o lo **metta in servizio**, indipendentemente dal fatto che sia a pagamento o gratuito e che **abbia sede nell'UE o fuori dall'UE**.

Questo soggetto è chiamato **FORNITORE**, che **può essere** a sua volta un **fabbricante del prodotto**, quando produce prodotti che incorporano sistemi di IA e utilizza il proprio nome o marchio. Anche il **FORNITORE**, con **sede** in un **Paese extra-UE**, il cui **sistema di IA genera informazioni di output da utilizzare nell'UE**, **deve rispettare il regolamento**.

INTRODUZIONE

Introduzione al mondo dell'Intelligenza Artificiale: i soggetti coinvolti

2. **Qualsiasi persona fisica o giuridica stabilita** o **situata** nell'**UE** che **utilizzi** un **sistema di IA sotto la propria autorità**, ad **eccezione** del **caso** in cui il suo **utilizzo** sia **solamente personale**, noto come **DEPLOYER**. Come i **FORNITORE**, anche i **DEPLOYER** di **sistemi di IA localizzati in un paese terzo**, sono **tenuti** a **rispettare** il **regolamento laddove l'output** prodotto dal sistema di IA **sia utilizzato nell'Unione**.

3. **altri soggetti** della catena di fornitura dei sistemi di IA, quali **importatori**, **DISTRIBUTORI** e **rappresentanti autorizzati di fornitori stabiliti nell'Unione**.

Il **Regolamento** deve essere **rispettato anche** da un **DISTRIBUTORE** stabilito o situato **al di fuori dell'UE**, **se** mette a disposizione un sistema di IA che **genera** un **output utilizzato nell'UE**.

2. **altre persone interessate** dai **sistemi di IA** che hanno **sede nell'Unione**.

6.3.2024 A9-0188/808

Emendamento 808
Anna Cavazzini
a nome della commissione per il mercato interno e la protezione dei consumatori
Juan Fernando López Aguilar
a nome della commissione per le libertà civili, la giustizia e gli affari interni

Relazione **A9-0188/2023**
Brando Benifei, Dragoş Tudorache
Regolamento sull'intelligenza artificiale
(COM(2021)0206 – C9-0146/2021 – 2021/0106(COD))

Proposta di regolamento
–

EMENDAMENTI DEL PARLAMENTO EUROPEO*

alla proposta della Commissione

REGOLAMENTO (UE) 2024/…
DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del ...

che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (legge sull'intelligenza artificiale)

(Testo rilevante ai fini del SEE)

SINTESI AI ACT :

400 pagine

180 considerando

113 ARTICOLI e 13 ALLEGATI

- **capo i disposizioni generali**
- **capo ii pratiche di IA vietate**
- **capo iii sistemi di IA ad alto rischio**
- **capo iv obblighi di trasparenza per i providers e i deployers**
- **capo v modelli di IA per finalità generali**
- **capo vi misure a sostegno dell'innovazione**
- **capo vii governance**
- **capo viii banca dati dell'UE per i sistemi ad alto rischio**
- **capo ix monitoraggio, condivisione, vigilanza**
- **capo x codici di condotta e orientamenti**
- **capo xi delega di potere e procedura di comitato**
- **capo xii sanzioni**

European Commission

REGOLAMENTO (UE) 2024/1689 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 13 giugno 2024 (c.d. AI Act)

- Noto come **AI ACT** stabilisce un **quadro normativo armonizzato** per lo **sviluppo**, **l'immissione** sul **mercato**, la **messa** in **servizio** e **l'uso** di **sistemi di intelligenza artificiale (IA) all'interno dell'unione europea.**
- Il **regolamento "AI ACT"** **modifica** e **integra** vari regolamenti e direttive precedenti per **garantire** che **l'IA** sia **utilizzata** **in conformità** con i **valori fondamentali dell'unione**, promuovendo una tecnologia **antropocentrica**, **affidabile** e **sicura**

A CHI SI APPLICA IL REGOLAMENTO SULL'IA?

- Il Regolamento (UE) 2024/1689 "AI ACT" si applica ai seguenti **soggetti**:

- **Fornitori** e **utilizzatori** (**deployer**) di IA **nell'Unione Europea**
- **Fornitori** e **utilizzatori** **extra UE** in cui **l'output** prodotto dai sistemi di IA è destinato a essere **utilizzato nell'Unione Europea**
- **Importatori** e **distributori** di **sistemi IA**
- Il regolamento "AI ACT" si applica ai sistemi di IA utilizzati nel territorio dell'Unione Europea. Tuttavia **non si applica** ai **sistemi IA** destinati a **scopi** **militari**, di **ricerca** e **sviluppo scientifici** o **usi non professionali.**

COS'È UN SISTEMA DI INTELLIGENZA ARTIFICIALE?

- Con **sistema di intelligenza artificiale (IA) si intende**

*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**.*

SISTEMA REGOLATIVO BASATO SUL RISCHIO

- **L'AI Act** adotta un **approccio basato sul rischio**, **classificando** i **sistemi** di **intelligenza artificiale** in **quattro categorie**:

- **Rischio inaccettabile**: tecnologie vietate del tutto.
- **Alto rischio**: soggette a rigide regolamentazioni e controlli.
- **Rischio limitato**: obbligo di trasparenza, ma con vincoli meno stringenti.
- **Rischio minimo**: nessuna restrizione particolare.

LE TAPPE DEL REGOLAMENTO EUROPEO AI ACT

- Queste le **date** di **applicazione** del **Regolamento 2024/1689 "AI ACT**:

- **01/08/2024**: **entrata in vigore del regolamento** (20 giorni dopo la pubblicazione nella G.U.)
- **02/02/2025**: diventano **applicabili** le **norme sulle pratiche di IA vietate**
- **02/08/2025**: si applicano le disposizioni relative alle **autorità di notifica nazionali individuate** e diventano **applicabili** i **modelli di IA per finalità generali**, la **governance**, le **sanzioni** (*escluse le sanzioni pecuniarie per i fornitori di modelli di IA per finalità generali*) e la **riservatezza** delle **informazioni**
- **02/08/2026**: **si applicano tutte le sezioni del regolamento**, ad **esclusione** di quanto previsto al **punto successivo**
- **02/08/2027**: sono **applicabili** gli **obblighi** per i **sistemi ad alto rischio**, prodotto o componente di un **di cui all'articolo 6**, paragrafo 1

IL REGOLAMENTO UE

- Si tratta di un **regolamento UE** e **non di una direttiva**;

Che differenze ci sono?

- **E' la prima regolamentazione al mondo sull'intelligenza artificiale**;

Come mai, siamo stati più solerti?

- **Non è un regolamento isolato** ma sarà **accompagnato** da **altri regolamenti** e **direttive**, **tutti volti a dare attuazione alla complessa strategia elaborata dalla commissione.**

Tanto che si parla di ecosistema

Es. Proposta di regolamento sui prodotti macchina,

Es. Proposta di direttiva sulla responsabilita' da intelligenza artificiale,

Es. Proposta nuova direttiva sulla responsabilita' per danno da prodotti difettosi,

DIFFERENZA TRA REOLAMENTO E DIRETTIVA

REGOLAMENTO UE (es. AI ACT)

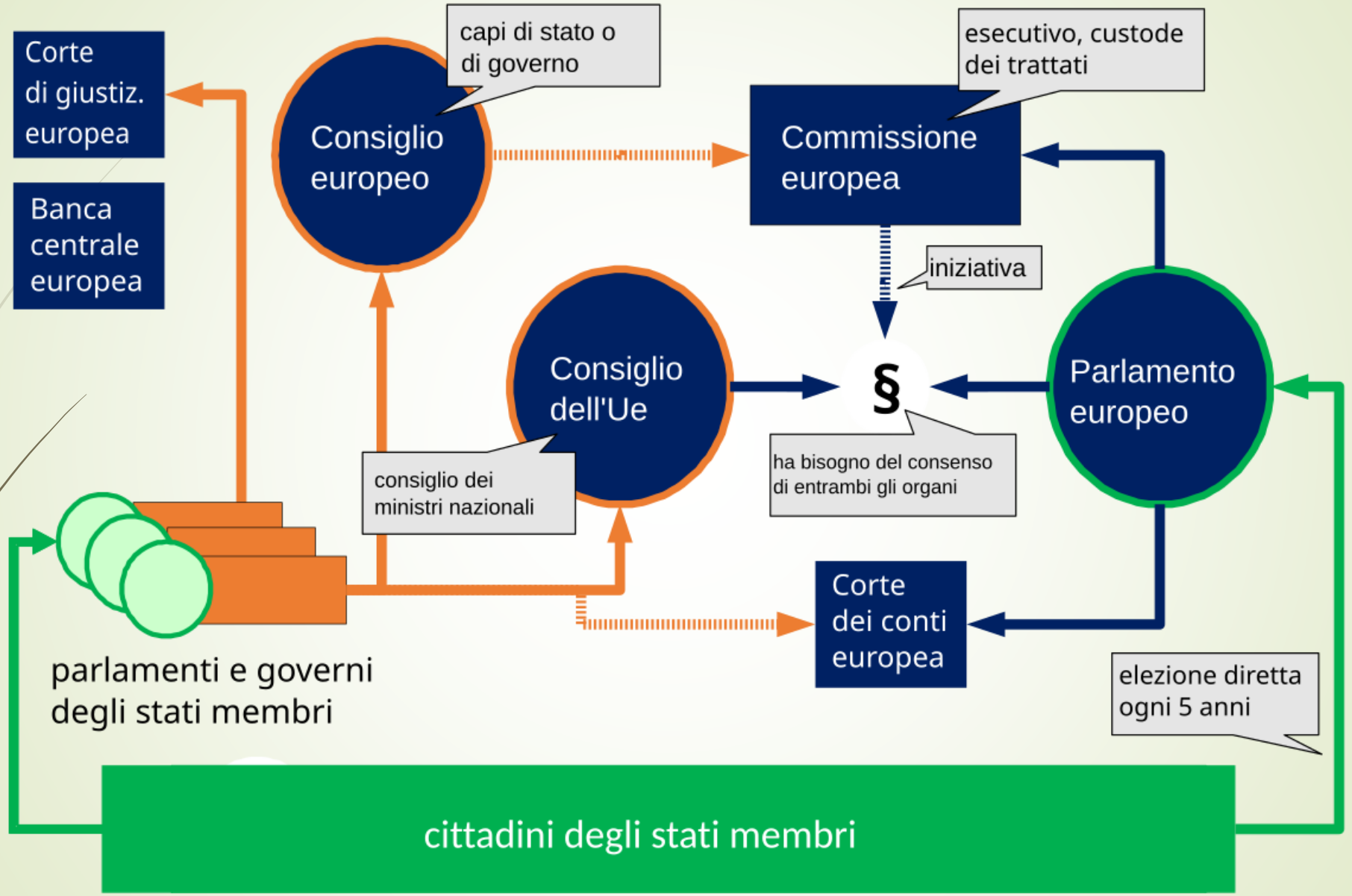
I **regolamenti** sono **atti giuridici** definiti *nell'**articolo 288 del trattato sul funzionamento dell'Unione europea (TFUE).*** Hanno portata generale, sono **vincolanti** **in tutti i loro elementi** e **direttamente applicabili** negli **Stati membri dell'Unione.**

- Hanno lo **scopo** di **garantire l'applicazione uniforme in tutta l'Unione della rispettiva normativa.**
- Un regolamento deve essere rispettato pienamente da coloro ai quali si applica ed è **direttamente applicabile negli Stati membri.** Ciò significa che:
- si applica direttamente negli Stati membri dopo la sua entrata in vigore, **senza richiedere il recepimento nel diritto nazionale**;

DIRETTIVA UE (es. NIS 2 cibersicurezza)

La **direttiva** è un atto giuridico, **vincola** gli **Stati membri della UE** per quanto riguarda il **risultato da raggiungere**, salvo **restando** la **competenza degli organi nazionali in merito alla forma e ai mezzi» (art. 288 par. 3 TFUE)**

- Persegue **l'obiettivo** di **armonizzare le normative degli Stati membri.**
- La direttiva **obbliga** gli Stati **membri** a un **determinato risultato**; il **legislatore nazionale** sceglierà i **mezzi** per ottenerlo è vincolante solo per quanto riguarda gli **obiettivi** **da conseguire**
- Il recepimento consiste nell'adozione di misure di portata nazionale al fine di **conformarsi** ai risultati che la direttiva prevede di raggiungere

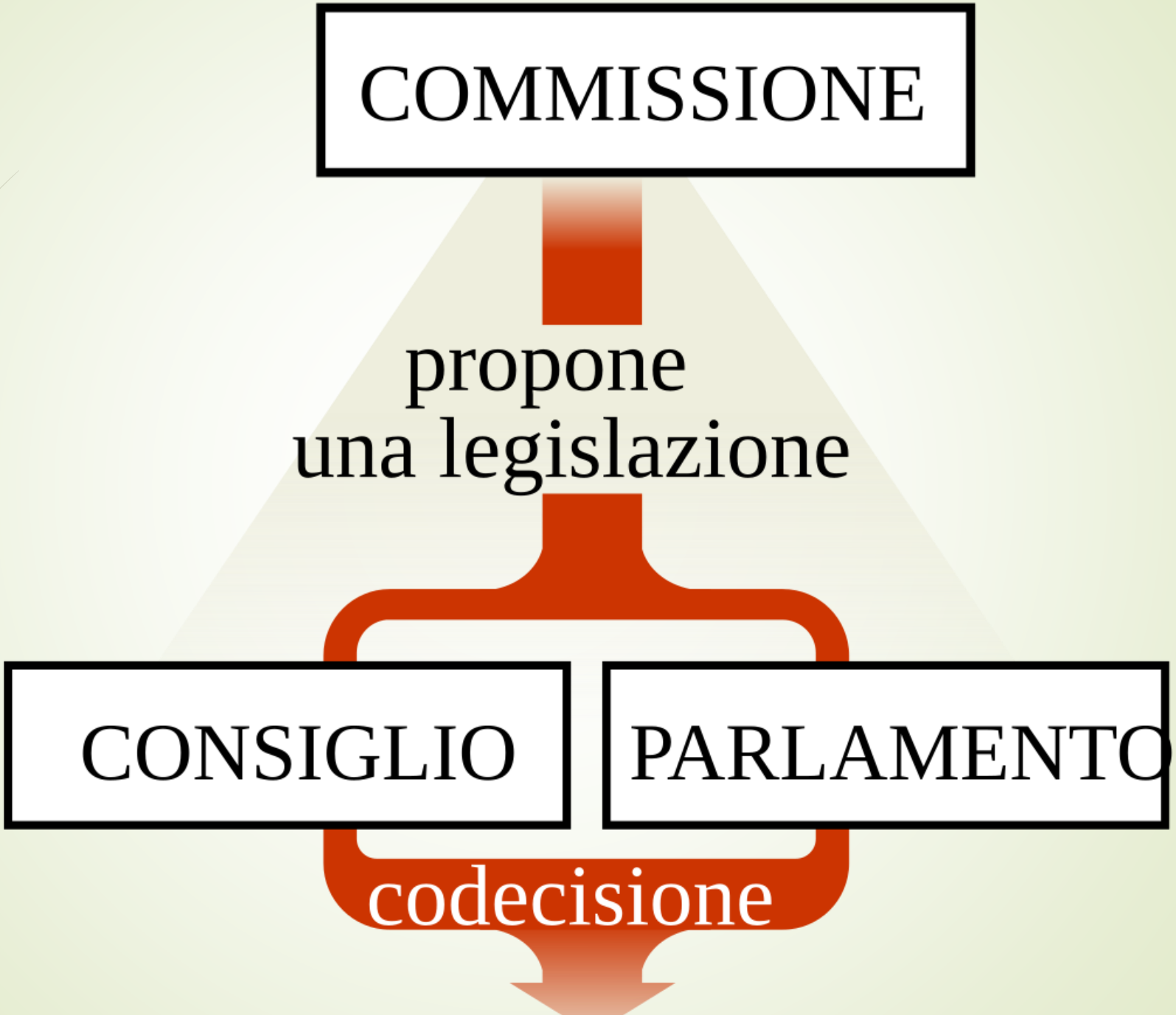

Corte di giustiz. europea
Banca centrale europea
Consiglio europeo
capi di stato o di governo
Commissione europea
esecutivo, custode dei trattati
iniziativa
Consiglio dell'Ue
§
Parlamento europeo
ha bisogno del consenso di entrambi gli organi
consiglio dei ministri nazionali
Corte dei conti europea
parlamenti e governi degli stati membri
elezione diretta ogni 5 anni
cittadini degli stati membri

LA COMMISSIONE EUROPEA

Le istituzioni dell'Unione europea sono sette:

- **il Parlamento europeo**,
- Il Consiglio europeo,
- il **Consiglio dell'Unione europea**,
- la **Commissione europea**,
- la Corte di giustizia dell'Unione europea,
- la Banca centrale europea,
- la Corte dei conti europea.

- La **Commissione europea** è una delle principali istituzioni dell'Unione europea, suo **organo esecutivo** e **promotrice del processo legislativo**. È composta da **delegati** (uno per ogni Stato membro dell'Unione europea, detto Commissario).
- **Rappresenta** e **tutela** gli **interessi dell'Unione europea** nella sua interezza e avendo il monopolio del potere di **iniziativa legislativa**, propone l'adozione degli atti normativi dell'UE, la cui approvazione ultima spetta al **Parlamento europeo** e al **Consiglio dell'Unione europea** (ministri);


COMMISSIONE
propone
una legislazione
CONSIGLIO
PARLAMENTO
codecisione

ITER IA ACT EU

LIBRO BIANCO

Il **percorso** che ha **portato all'elaborazione** del **regolamento** da parte della **commissione** aveva avuto inizio a partire dal **2017**, nella **consapevolezza dell'urgenza di dover far fronte alle tendenze emergenti**:

la **commissione** ha dapprima **elaborato**:

- -la **strategia europea sull'intelligenza artificiale**;
- il **libro bianco sull'intelligenza artificiale**,

in cui:

- si sono **definiti caratteri fondamentali** dell'approccio **UE sull'AI;**
- dato **avvio** alle **consultazioni con gli stakeholder**

Lo **stakeholder** (inglese, lett. "**portatore di bastone**") o **portatore di interesse** è un **soggetto** o gruppo, **coinvolto in un'iniziativa**, società o altro progetto, e con **interessi** legati all'esecuzione o dall'andamento dell'iniziativa stessa.

- si e' giunti all' **elaborare** la **proposta** di **Regolamento** del **2021** di **ai act** .

AI ACT PARTE DI UN ECOSISTEMA

Non e' un regolamento isolato ma **sara' accompagnato da altri regolamenti e direttive**, tutti volti a dare **attuazione** alla **complessa strategia elaborata dalla commissione.**

es. proposta di regolamento sui *prodotti macchina*,

es. proposta di direttiva sulla *responsabilita'* da *intelligenza artificiale*,

es. proposta nuova direttiva sulla *responsabilita'* per *danno da prodotti difettosi*,

ITER AI ACT EU

Regolamento (UE) 2021/0106

- La **Commissione europea** ha presentato la **proposta** per l'adozione del **Regolamento (UE) 2021/0106**

- Stabilisce **regole armonizzate sull'intelligenza artificiale**

- **In linea** con gli **orientamenti politici dichiarati del presidente la commissione** (2019-2024) Ursula Von der Leyen

Obiettivo

- **Promuovere uno sviluppo etico dell'intelligenza artificiale**, in linea con i **valori fondamentali dell'unione europea**

- Garantire il **ruolo di leader all' UE nel panorama delle nuove tecnologie,** non tanto da un punto di vista tecnologico (*Usa e Cina sono molto piu avanzate*) , ma da un **punto di vista normativo**, **rafforzando** al **contempo la fiducia dei cittadini**

- **l'ambizione** è quella di creare la **prima regolamentazione al mondo sulli' IA** in modo da **influenzare** le **scelte degli altri paesi** attraverso la **propria regolamentazione** (anche con la diffusione dei **modelli di fondazione**)

Perché un regolamento e non una direttiva

- La scelta è' abbastanza comprensibile, tenendo conto della **dimensioni** del **fenomeno** ben si **comprende** la scelta di intervenire in maniera **coordinata** a livello **europeo**, **evitando azioni autonome** da parte dei **singoli stati membri**

- Il **regolamento** difatti, a differenza della direttiva, e' **idoneo a garantire immediata** ed **uniforme applicazione** su **tutto** il **territorio dell'unione**

ITER AI ACT EU

Nell'elaborazione finale del **Regolamento** uno dei **problemi principali** ha riguardato:

LA REGOLAMENTAZIONE DEI MODELLI DI FONDAZIONE

alcuni paesi: Italia, Germania e Francia hanno manifestato la loro **contrarietà all'approccio REGOLAMENTARE** adottato nel **REGOLAMENTO (UE) 2021/0106**, rispetto ai **modelli di fondazione**, ritenendo che le **regole previste troppo stringenti**, ponendo così di fatto un **FRENO** allo **SVILUPPO** e agli **INVESTIMENTI**.
Contrapposisizione tra:

POTENZIALI RISCHI E PER L'IMPATTO SUI DIRITTI FONDAMENTALI

TIMORE CHE REGOLE TROPPO STRINGENTI AVREBBERO RAPPRESENTATO UN FRENO ALLO SVILUPPO

COSA SONO I MODELLI DI FONDAZIONE

- Nel **2021**, un gruppo di **studiosi dell'Università di Stanford** introdusse il **termine** "**foundation models**" nel **report** «***On the Opportunities and Risks of Foundation Models»,***
- Nell'ambito **dell'Intelligenza Artificiale (IA)**, con il termine "**modello**" si fa riferimento a un **insieme strutturato di algoritmi e parametri** che permettono di eseguire **specifici compiti** di **apprendimento automatico**. I **modelli** sono **addestrati** tramite **l'analisi** e **l'elaborazione** di **dati**, al fine di **identificare** e **apprendere schemi** o **relazioni** tra di **essi**.
- Un **foundation model** rappresenta un **tipo specifico e avanzato** di **modello** di **Intelligenza Artificiale**.

- I ***modelli "generici*** di **Intelligenza Artificiale** sono **progettati** e **addestrati** per svolgere **compiti specifici** e **ben definiti** e possono essere addestrati su **set di dati** di **dimensioni variabili**, a seconda del compito che dovranno svolgere.
- I **foundation models**, invece, sono **addestrati** su **enormi quantità di dati** e con **moltissimi parametri**. Ciò permette loro di svolgere una **varietà di compiti più ampia rispetto** ai **modelli tradizionali.**
- I **foundation models** possono dunque essere **definiti** come "**modelli di base di grandi dimensioni**". "**Di base**" perché, grazie alla loro **capacità** di **svolgere diversi compiti**, fungono da "**fondamenta**" o **punto di partenza** per lo **sviluppo di sistemi avanzati**.

COSA SONO I MODELLI DI FONDAZIONE

- **Esempi** attuali di **foundation models** sono **GPT-3 e 4** di **OpenAI** e **BERT** di **Google**. Per avere un'idea della dimensione e della **rapida evoluzione** di questi **modelli**, basti pensare che **GPT-3**, rilasciato nel **giugno 2020**, **utilizza 175 miliardi di parametri**, mentre **GPT-4**, rilasciato nel **marzo 2023**, ben **100 trilioni**.
- Le **principali caratteristiche** dei **foundation models** si possono riassumere in emersione e omogeneizzazione.

Emersione

Nel ***report*** si legge che **emersione** "***significa*** *che il* ***comportamento di un sistema è implicitamente indotto*** *piuttosto che* ***esplicitamente costruito***". Ciò **indica** che molte **capacità** di questi **modelli** **emergono** durante il **processo** di **addestramento** senza che vengano espressamente programmate.

In altre parole, i **foundation models** sono **capaci** di **apprendere compiti complessi** e **specifici** **non perché siano stati progettati in modo esplicito** per svolgerli, **ma** perché hanno **analizzato e processato enormi quantità di dati**, **acquisendo** in modo **autonomo** **determinate capacità.**

Omogeneizzazione

I **foundation models** sono **progettati** per essere altamente **generalisti** in modo da poter essere **utilizzati** in **molti contesti** e per **molteplici applicazioni.** Questo significa che essi **omogeneizzano**, o **rendono uniformi**, le **capacità** di varie **applicazioni** di **Intelligenza Artificiale**. **Invece** di avere *diversi modelli piccoli e specializzati*, **c'è** un **unico, grande modello** che può essere **adattato** a **vari compiti**.

COSA SONO I MODELLI DI FONDAZIONE

Possibili rischi

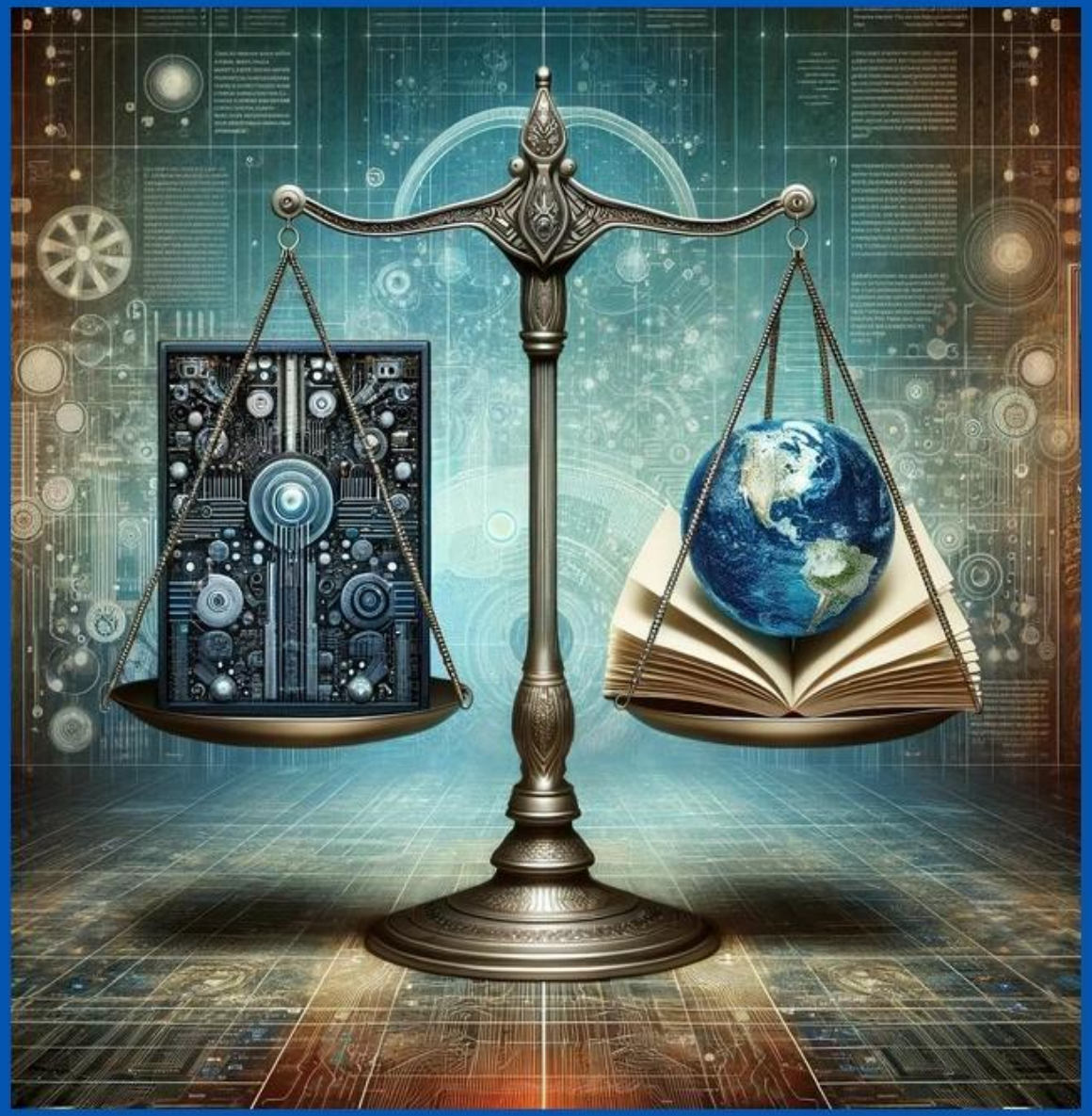
Emersione ed **omogeneizzazione** sono **caratteristiche incredibili** che evidenziano il **progresso** in **questo settore** e le **sue potenzialità future**, **ma portano** anche dei **rischi**.

- L'**omogeneizzazione** può essere **vantaggiosa** in settori con **scarsità** di **dati disponibili** (come **sanità** e , a **causa** delle normative sulla **privacy**), in quanto **permette l'uso** di modelli **generalisti** in diversi contesti. Tuttavia, questo **comporta** anche che **difetti**, **imprecisioni**, ed **errori** del **modello originario** possano essere **trasferiti** a **tutti i modelli derivati**, sollevando **problemi etici e di equità**.
- Riguardo all'**emersione**, se da un lato rappresenta la "**forza**" e il **principale vantaggio di questi modelli**, dall'altro lato ne **complica l'interpretazione**, la **valutazione** e la **previsione**. Tale **mancanza di trasparenza** e **comprensibilità può generare criticità** in termini di **sicurezza.**

- Tra le **numerose applicazioni** dei **foundation models**, gli autori del **report *On the Opportunities and Risks of Foundation Models*** scelgono di focalizzarsi su **tre settori cruciali**: **sanità**, **diritto** ed **educazione**.
- Nella **sanità**, i foundation models promettono di **superare** le **limitazioni** legate alla **scarsità dei dati**, permettendo l'analisi di diverse tipologie di informazioni, dai testi alle strutture molecolari. Tuttavia, esiste il **pericolo** di perpetuare possibili **pregiudizi storici presenti** nei **dati medici**.
- Nel **diritto**, **l'abbondanza** di **documenti legali** rende **ideale l'utilizzo** di questi **modelli**, che potrebbero rivoluzionare la **creazione** e **l'analisi** dei **testi giuridici**. **L'importanza della veridicità** delle **informazioni generate** non può però essere **sottovalutata**. **Pericolo** di **allucinazioni.**
- Nel **settore educativo**, i foundation models possono **sfruttare diverse fonti**, come **libri di testo** e **video**, per **supportare l'apprendimento.** Offrono **benefici** come la **generazione di esercizi** e **feedback personalizzati**, ma presentano anche **rischi** quali problemi di **privacy**, **possibilità di plagio.**

L'approccio europeo all'Intelligenza artificiale:

l' ecosistema dell'eccellenza e l'ecosistema della fiducia



QUATTRO OBIETTIVI POLITICI CHIAVE PER L'INTELLIGENZA ARTIFICIALE IN EUROPA

CREARE LE CONDIZIONI PER LO SVILUPPO E L'UTILIZZO DELL'IA NELL'UE

- Acquisire, aggregare e condividere informazioni sulle politiche
- Sfruttare il potenziale dei dati
- Promuovere essenziali capacità di computing

FARE DELL'UE IL LUOGO IDONEO: ECCELLENZA DAL LABORATORIO AL MERCATO

- Collaborazione con le parti interessate, partenariato pubblico-privato su AI, dati e robotica
- Capacità di ricerca
- Test e sperimentazione (TEF), adozione da parte delle PMI (EDIH)
- Finanziamento e scalabilità di idee e soluzioni innovative

ASSICURARE CHE LE TECNOLOGIE IA FUNZIONINO PER LE PERSONE

- Talento e competenze
- Un quadro di politiche per garantire la fiducia nei sistemi di intelligenza artificiale
- Promuovere la visione dell'UE su un'IA sostenibile e affidabile nel mondo

COSTRUIRE UNA LEADERSHIP STRATEGICA IN ALCUNI SETTORI

- Clima e ambiente
- Salute
- Strategia per la robotica nel mondo dell'IA
- Settore pubblico
- Forze dell'ordine, immigrazione e asilo
- Mobilità
- Agricoltura

6.3.2024 A9-0188/808

Emendamento 808
Anna Cavazzini
a nome della commissione per il mercato interno e la protezione dei consumatori
Juan Fernando López Aguilar
a nome della commissione per le libertà civili, la giustizia e gli affari interni

Relazione **A9-0188/2023**
Brando Benifei, Dragoş Tudorache
Regolamento sull'intelligenza artificiale
(COM(2021)0206 – C9-0146/2021 – 2021/0106(COD))

Proposta di regolamento
–

EMENDAMENTI DEL PARLAMENTO EUROPEO*

alla proposta della Commissione

REGOLAMENTO (UE) 2024/…
DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del ...

che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (legge sull'intelligenza artificiale)

(Testo rilevante ai fini del SEE)

SINTESI AI ACT :

400 pagine

180 considerando

113 ARTICOLI e 13 ALLEGATI

- **capo i disposizioni generali**
- **capo ii pratiche di IA vietate**
- **capo iii sistemi di IA ad alto rischio**
- **capo iv obblighi di trasparenza per i providers e i deployers**
- **capo v modelli di IA per finalità generali**
- **capo vi misure a sostegno dell'innovazione**
- **capo vii governance**
- **capo viii banca dati dell'UE per i sistemi ad alto rischio**
- **capo ix monitoraggio, condivisione, vigilanza**
- **capo x codici di condotta e orientamenti**
- **capo xi delega di potere e procedura di comitato**
- **capo xii sanzioni**

European Commission

AI ACT : concetti chiave

- Coordinamento
- Regolamentazione
- Investimenti

Regole "classiche" del mercato interno per l'immissione sul mercato e la messa in servizio dei sistemi di IA

Approccio basato sul rischio

Nessuna regolamentazione della tecnologia in quanto tale ma dei casi d'uso concreti ad alto rischio

Parità di condizioni per operatori UE e non-UE

Catalizzare investimenti attraverso programmi UE (DIGITAL EUROPE, HORIZON EUROPE, PNRR)

Scopo dell'AI ACT (art. 1 AI ACT)

«Lo scopo del presente regolamento è migliorare il ***funzionamento del mercato interno*** *e promuovere la diffusione di* ***un'intelligenza artificiale antropocentrica e affidabile****, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali, compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, contro gli effetti nocivi dei sistemi di intelligenza artificiale nell'Unione nonché promuovere l'innovazione»*

AMBITO DI APPLICAZIONE

Soggetti coinvolti

- L'IA Act identifica **tre principali categorie** di **attori:**

1. **FORNITORI**

Sono i soggetti che **sviluppano**, **progettano** o **mettono sul mercato** sistemi di IA. Questi attori **devono**:

- **Garantire** che i sistemi rispettino i requisiti essenziali di sicurezza e trasparenza.
- **Condurre** valutazioni del rischio e audit.
- **Fornire** documentazione tecnica e garanzie di conformità.

2. UTILIZZATORI per scopi professionali

(DEPLOYER)

Riguarda chi utilizza i sistemi di IA per scopi professionali o operativi. Gli utilizzatori **devono**:

- **Impiegare i sistemi in modo** conforme alle istruzioni dei fornitori.
- Monitorare **continuamente l'uso** per identificare eventuali rischi.

3. DISTRIBUTORI e IMPORTATORI

- Questi sono **intermediari** che **mettono a disposizione** o **distribuiscono** sistemi di IA **sviluppati da altri soggetti**. Hanno l'obbligo di **verificare** che i **prodotti** rispettino i requisiti dell'IA Act prima di **immetterli sul mercato** europeo.

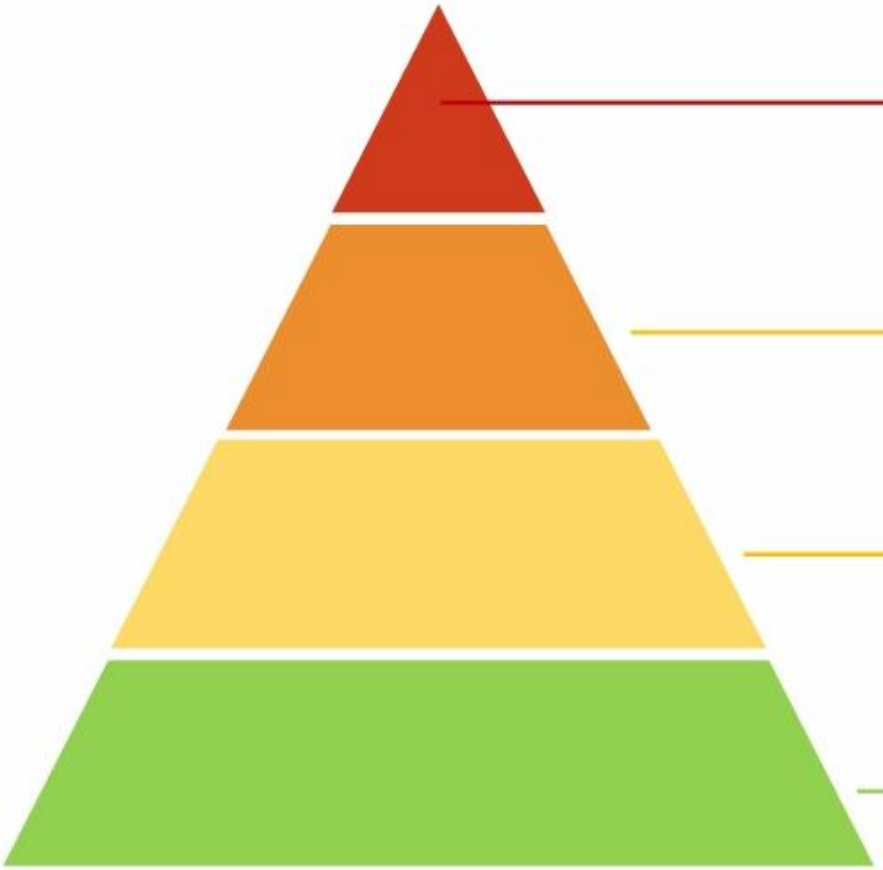
APPLICAZIONE IN BASE ALLA CLASSIFICAZIONE DEI RISCHI

- Al fine di voler **regolamentare l'utilizzo** e la **diffusione** dei **sistemi di IA**, **senza frenarne lo sviluppo**, ha portato alla costruzione di una
- **normativa orizzontale** (**applicabile a tutti i sistemi di ia**)

e

- **a strati** (**che impone obblighi differenziati**), **sulla base** del **livello di rischio attribuito** ai diversi sistemi.
- IL **CONCETTO DI RISCHIO** è definito **all'art. 3 , n. 2) dell'AI ACT** come: «**LA COMBINAZIONE DELLA PROBABILITA' DEL VERIFICARSI DI UN DANNO E LA GRAVITA' DELLO STESSO».**

Un approccio regolamentare basato sul rischio



Rischio non accettabile
es. punteggio/credito sociale

Proibito

Rischio alto
es. reclutamento, dispositivi medici

Permesso soggetto a conformità con requisiti per l'IA e una valutazione della conformità ex-ante.

IA con specifici rischi legati alla trasparenza
'Impersonificazione' (bots)

Permesso ma soggetto a obblighi di informazione/trasparenza

Rischi minimi o assenti

Permesso senza restrizioni

European Commission

APPLICAZIONE IN BASE ALLA CLASSIFICAZIONE DEI RISCHI – RISCHIO INACCETTABILE

A. Rischio inaccettabile (SISTEMI PROIBITI)

Articolo 5

- 1. Sono vietate le pratiche di IA seguenti: **Pratiche di IA vietate**

Comprendono tecnologie che rappresentano una **minaccia significativa** per i **DIRITTI FONDAMENTALI**, **LIBERTA DELLE PERSONE**, **CONTRARIETA' AI VALORI FONDANTI DELL'UE** (dignità umana, libertà, uguaglianza , democrazia e principio di diritto). **Indipendentemente** delle **ipotesi previste dall'art. 5** il **divieto vale ogniqualvolta è contrario ai valori fondanti della UE.**

APPLICAZIONE IN BASE ALLA CLASSIFICAZIONE DEI RISCHI – RISCHIO INACCETTABILE

A. Rischio inaccettabile (SISTEMI PROIBITI)

È importante chiarire che **l'IA Act adotta una regolamentazione basata su livelli di rischio**, per cui **non è la tecnologia in sé a essere regolamentata**, ma i **suoi usi concreti**.

- Partendo da questa premessa, **l'IA Act vieta l'uso di sistemi di intelligenza artificiale** per determinati **scopi** considerati **minacce** **per la** **sicurezza**, la **vita** e i **diritti delle persone**. I sistemi vietati includono:

1) **Sistemi che utilizzano tecniche subliminali o manipolative**, in grado di influenzare significativamente il comportamento di una persona, compromettendone la capacità di prendere decisioni informate e causando potenziale danno a sé stessa o a terzi.
2) **Sistemi che sfruttano le vulnerabilità di una persona** per influenzare il suo comportamento, con il rischio di provocare danno a sé stessa o a terzi.
3) **Sistemi di valutazione o classificazione sociale**, come il **social scoring (usato in Cina)** , che possono comportare trattamenti discriminatori o sfavorevoli per alcune persone o gruppi.
4) **Sistemi di valutazione del rischio di criminalità**, basati sulla **profilazione** o su caratteristiche personali.
5) **Raccolta massiva di immagini facciali online o tramite CCTV** (tv circuito chiuso – videosorveglianza) per il riconoscimento facciale.
6) **Sistemi di riconoscimento delle emozioni** da usare in ambito lavorativo o educativo.

APPLICAZIONE IN BASE ALLA CLASSIFICAZIONE DEI RISCHI - RISCHIO INACCETTABILE

1) Rischio inaccettabile (SISTEMI PROIBITI)

7) **Sistemi di categorizzazione biometrica** basati su caratteristiche sensibili come razza, opinioni politiche, religione o orientamento sessuale.
8) **Sistemi di identificazione biometrica in tempo reale in luoghi pubblici**, eccetto per scopi di ricerca selettiva, prevenzione di minacce imminenti o identificazione di sospetti di reati penali.

APPLICAZIONE IN BASE ALLA CLASSIFICAZIONE DEI RISCHI – SISTEMI AD ALTO RISCHIO

B. Sistemi ad alto rischio

La **qualificazione** di **sistema ad alto rischio** è particolarmente **rilevante** in quanto ne **discendono** una **serie di obblighi stringenti**.

Classificazione dei sistemi di IA come «ad alto rischio»

L' Articolo 6 fissa le Regole di classificazione per i sistemi di IA ad alto rischio

1. A prescindere dal fatto che sia immesso sul **mercato** o messo in **servizio** indipendentemente dai prodotti di cui alle lettere a) e b), un **sistema di IA** è considerato ad **alto rischio se** sono **soddisfatte entrambe le condizioni seguenti: a)** il **sistema di IA** è destinato a essere utilizzato come componente di sicurezza di un prodotto, o il sistema di IA è esso stesso un prodotto, **disciplinato dalla normativa di armonizzazione dell'Unione elencata nell'allegato I; b)** il **prodotto**, il cui componente di sicurezza a norma della lettera a) è il sistema di IA, o il sistema di IA stesso in quanto prodotto, è **soggetto** a una **valutazione** della conformità da parte di **terzi** ai fini **dell'immissione** sul **mercato** o della messa in **servizio** di tale prodotto ai sensi della normativa di armonizzazione dell'Unione elencata **nell'allegato I.**

APPLICAZIONE IN BASE ALLA CLASSIFICAZIONE DEI RISCHI – SISTEMI AD ALTO RISCHIO

B. Sistemi ad alto rischio

L'articolo 6 stabilisce le **regole generali** per determinare se un **sistema di IA è considerato ad alto rischio.** In particolare, si basa su due criteri:

1. **Componenti di sicurezza in prodotti regolamentati art. 6**

- Se un **sistema di IA è utilizzato come componente di sicurezza di un prodotto regolato da leggi europee preesistenti** (**elencate nell'allegato I**) **e** il **prodotto stesso** è **soggetto** a **valutazione di conformità da parte di terzi**, **allora l'IA è considerata ad alto rischio.**

2. **Sistemi** elencati **nell'allegato III**

- Se un **sistema di IA** rientra nei **casi specificati nell'allegato III**, è automaticamente classificato come ad alto rischio.

APPLICAZIONE IN BASE ALLA CLASSIFICAZIONE DEI RISCHI – SISTEMI AD ALTO RISCHIO

B. Sistemi ad alto rischio

Un sistema di intelligenza artificiale (AI) è considerato **ad alto rischio quando** il **suo utilizzo può** avere un **impatto significativo** sulla **sicurezza**, sui **diritti fondamentali** o sul **benessere** delle **persone**. Secondo il **Regolamento sull'AI dell'Unione Europea (AI Act)**, un sistema è classificato come **ad alto rischio** se **rientra in una delle seguenti categorie:**

1. Sistemi AI in ambiti critici

Questi sono **contesti** in cui un **errore dell'AI** potrebbe avere **conseguenze gravi**:

- **Sicurezza e infrastrutture critiche** (es. **gestione** delle **reti energetiche**, **trasporti pubblici**).
- **Sanità** (es. **diagnostica medica assistita da AI, robot chirurgici**).
- **Istruzione e formazione** (es. **valutazione automatizzata degli studenti, selezione per corsi**).
- **Occupazione e risorse umane** (es. **strumenti di reclutamento, valutazione delle performance**).
- **Servizi pubblici e giustizia** (es. **decisioni amministrative automatizzate, AI nei tribunali**).

APPLICAZIONE IN BASE ALLA CLASSIFICAZIONE DEI RISCHI – SISTEMI AD ALTO RISCHIO

B. Sistemi ad alto rischio

2. Sistemi AI che influenzano i diritti fondamentali

Questi includono **tecnologie** che possono **incidere su privacy,** non discriminazione e libertà individuale, come:

- **AI per la sorveglianza biometrica** (es. **riconoscimento facciale in spazi pubblici**).
- **AI nei servizi finanziari** (es. **valutazione del credito, assicurazioni**).
- **Sistemi AI per l'applicazione della legge** (es. **previsione criminale, analisi dei rischi**).
- **AI nella migrazione e nelle frontiere** (es. **sistemi per il controllo automatico dei visti**)

APPLICAZIONE IN BASE ALLA CLASSIFICAZIONE DEI RISCHI – SISTEMI AD ALTO RISCHIO

B. Sistemi ad alto rischio

3. Eccezioni: Un **sistema di IA elencato nell'allegato III può non essere considerato ad alto rischio se non** presenta un **rischio significativo per** la salute, la sicurezza o i diritti fondamentali delle persone fisiche, anche nel caso in cui non influenzi materialmente il risultato del processo decisionale. Questa deroga si **applica** quando è **soddisfatta almeno una delle seguenti condizioni:**

- Il sistema di IA è destinato a eseguire un **compito procedurale limitato**;
- Il sistema di IA è destinato a **migliorare il risultato di un'attività umana precedentemente completata**;
- Il sistema di IA è destinato a **rilevare schemi decisionali o deviazioni da schemi decisionali precedenti e non è finalizzato a sostituire o influenzare la valutazione umana precedentemente completata senza un'adeguata revisione umana;**
- Il sistema di IA è destinato a eseguire un **compito preparatorio per una valutazione pertinente ai fini dei casi d'uso elencati nell'allegato III.**

➨ Tuttavia, un **sistema di IA** che effettua la **profilazione** di **persone fisiche** è **sempre considerato ad alto rischio.**

APPLICAZIONE IN BASE ALLA CLASSIFICAZIONE DEI RISCHI – SISTEMI AD ALTO RISCHIO

I sistemi di IA ad alto rischio allegato I allegato III.

B. Sistemi ad alto rischio

Allegato I riporta vari **Regolamenti** riguardanti **settori critici**, i **più significativi sono**: (entrano in vigore dal 2 agosto 2027)

- **Sanità** (dispositivi medico-diagnostici in vitro, dispositivi medici).
- **Regolamento macchine**

Allegato III riporta vari **Regolamenti** riguardanti **settori critici come**: (entrano in vigore dal 2 agosto 2026)

- **Istruzione** (sistemi di valutazione automatizzati).
- **Lavoro** (strumenti di selezione del personale).

- I **settori indicati dall'allegato III non sono tassativi**, i **fornitori possono essere esentatati dai vincoli se dimostrano che non sono un rischio significativo per salute, sicurezza, diritti fondamentali**,
- **L'allegato III** puo essere **modificato** anche dalla **Commissione**, **aggiungendo altre categorie ritenute a rischio per salute, sicurezza, diritti fondamentali.**

APPLICAZIONE IN BASE ALLA CLASSIFICAZIONE DEI RISCHI – SISTEMI AD ALTO RISCHIO

Sistemi ad alto rischio

- L'Allegato III del regolamento identifica una **serie di categorie di IA considerate ad alto rischio**, poiché possono comportare **effetti pregiudizievoli** per la **salute**, la **sicurezza** o i **diritti fondamentali delle persone**. Questi **sistemi di IA devono soddisfare specifici requisiti** per poter essere **introdotti** nel **mercato europeo**.

A) Categorie di sistemi ad alto rischio

I sistemi di IA ad alto rischio comprendono quelli impiegati nei seguenti ambiti: (all. n. III)

- a) **Componenti di sicurezza di un prodotto** regolamentato come macchinari, giocattoli, veicoli, dispositivi sanitari, apparecchi radio, attrezzature di protezione e altri prodotti con specifiche regolamentazioni europee.
- b) **Sistemi di identificazione biometrica remota** per identificare persone (esclusi i sistemi di autenticazione biometrica che verificano l'identità dichiarata).
- c) **Componenti di infrastrutture critiche** (es. traffico, gestione di acqua, gas, elettricità).
- d) **Sistemi per istruzione e formazione professionale** che possono influenzare l'accesso all'istruzione e le carriere.

APPLICAZIONE IN BASE ALLA CLASSIFICAZIONE DEI RISCHI – SISTEMI AD ALTO RISCHIO

- e) **Sistemi per il reclutamento e gestione delle risorse umane**, come la selezione di candidati e la valutazione delle performance lavorative.
- f) **Sistemi per l'accesso a servizi pubblici e privati essenziali**, come il credito e i servizi di assistenza.
- g) **Sistemi per forze di sicurezza**, come poligrafi e strumenti di analisi forense.
- h) **Sistemi per l'amministrazione della giustizia** e i processi democratici.

APPLICAZIONE IN BASE ALLA CLASSIFICAZIONE DEI RISCHI – SISTEMI AD ALTO RISCHIO

Se un fornitore ritiene che un sistema di IA non sia ad alto rischio, dovrà:

- a) **Redigere** una **valutazione** di **conformità documentata** prima della sua immissione sul mercato, per dimostrare la conformità ai requisiti dell'UE.
- b) **Registrare** il **sistema** nella **banca dati dell'UE** come previsto **dall'art. 71** del regolamento.

APPLICAZIONE IN BASE ALLA CLASSIFICAZIONE DEI RISCHI - SISTEMI AD ALTO RISCHIO

c) **Requisiti per i sistemi di IA ad alto rischio**

- Se un **sistema** viene **classificato** come ad **alto rischio**, il **fornitore** **deve** rispettare i **requisiti** indicati negli **articoli 8-15 dell'IA Act**, adattandosi alla **finalità d'uso** e allo **stato dell'arte**.

APPLICAZIONE IN BASE ALLA CLASSIFICAZIONE DEI RISCHI – SISTEMI AD ALTO RISCHIO

Quando un **sistema di IA** è valutato come ad **alto rischio**, i **soggetti coinvolti devono rispettare le disposizioni stabilite dall'AI Act**. In particolare, i **fornitori** devono **garantire** il **rispetto** della **maggioranza** degli **obblighi previsti dalla normativa**, nonché la corretta implementazione e gestione del sistema.

I. Obblighi dei FORNITORI

Il regolamento stabilisce che i provider di sistemi di IA ad alto rischio debbano garantire una serie dettagliata di requisiti, tra cui:

1. **Sistema di gestione dei rischi**: Durante l'intero ciclo di vita del sistema, questo dovrà essere oggetto di revisioni e **controlli periodici** per **identificare** e **analizzare** i **rischi conosciuti** e **prevedibili**, nonché **i potenziali rischi derivanti da un utilizzo improprio o inappropriato** della tecnologia.
2. **Modello di governance dei dati**: È necessario **adottare** e **mantenere standard elevati** di **qualità** e **governance** dei **dati**. Questi devono focalizzarsi principalmente sulla definizione di procedure di governance e gestione dei dati conformi alla finalità del sistema, **garantendo** che il **sistema** sia **pertinente**, **rappresentativo**, **privo di errori**, **completo** e **adeguato** al **contesto di utilizzo**.

APPLICAZIONE IN BASE ALLA CLASSIFICAZIONE DEI RISCHI – SISTEMI AD ALTO RISCHIO

3. **Documentazione tecnica dettagliata**: **Prima** che il **sistema sia immesso sul mercato**, il **fornitore** **deve** elaborare una **documentazione tecnica** che includa quanto **richiesto nell'allegato IV dell'AI Act**. La documentazione deve contenere almeno le seguenti informazioni:

1. **Descrizione generale del sistema di IA**, comprensiva delle **finalità** a cui è destinato, una descrizione di base dell'interfaccia utente fornita all'utilizzatore o deployer, e le relative **istruzioni per l'uso.**
2. **Descrizione dettagliata degli elementi costitutivi del sistema**, incluse le misure di sorveglianza umana e le misure di cibersicurezza implementate.
3. **Monitoraggio, funzionamento e controllo**: informazioni sulle capacità e limitazioni del sistema, compresi possibili risultati indesiderati e le fonti di rischio per la salute, la sicurezza e i diritti fondamentali.
4. **Idoneità delle metriche di prestazione**: descrizione delle metriche utilizzate per valutare il funzionamento del sistema.
5. **Gestione dei rischi**: descrizione dettagliata delle **procedure di gestione dei rischi**.
6. **Modifiche nel ciclo di vita del sistema**: **registrazione** delle **modifiche apportate durante il ciclo di vita** del sistema.
7. **Elenco degli standard seguiti**: indicazione degli **standard adottati** durante lo sviluppo e l'implementazione.
8. La **documentazione** dovrà essere **messa a disposizione** degli **utilizzatori**.

APPLICAZIONE IN BASE ALLA CLASSIFICAZIONE DEI RISCHI - SISTEMI AD ALTO RISCHIO

4. **Garanzia della tracciabilità** I sistemi dovranno consentire la **registrazione automatica dei log e la loro conservazione,** al fine di istituire un sistema di **monitoraggio post-commercializzazione** e per identificare **possibili rischi** derivanti dalla qualifica di prodotto ad alto rischio.
5. **Soddisfare un livello adeguato di accuratezza, robustezza e sicurezza informatica** I sistemi devono essere progettati per raggiungere un **livello adeguato di accuratezza**, **robustezza** e **sicurezza informatica**, riducendo il rischio di malfunzionamenti e vulnerabilità informatiche.
6. **Supervisione umana** È necessario prevedere una **supervisione umana durante il funzionamento del sistema**, **non solo per monitorare** la funzionalità, ma **anche** per **intervenire** **in caso di malfunzionamenti** o situazioni impreviste.
7. **Valutazione della conformità** e **dimostrazione della conformità** I **fornitori** di sistemi ad alto rischio **devono sottoporsi a una valutazione della conformità ai requisiti dell'AI Act**. A seconda della tipologia di sistema, la valutazione può essere basata su **controlli interni** (che non richiedono l'intervento di autorità regolatorie) **o** su un **sistema di gestione della qualità e documentazione tecnica che prevede l'intervento di un'autorità di regolamentazione.**
8. **Monitoraggio post-commercializzazione** È necessario **istituzionalizzare un sistema di monitoraggio** continuo del sistema, per **raccogliere dati sugli eventuali rischi o problematiche emerse una volta che il sistema è stato immesso sul mercato.**
9. **Registrazione** I **sistemi di IA ad alto rischio devono essere registrati presso le autorità dell'UE prima** di essere **immessi sul mercato o messi in servizio**. Questa registrazione è **obbligatoria anche** se il sistema, pur rientrando tra quelli ad alto rischio, può essere **escluso dalle eccezioni.**

APPLICAZIONE IN BASE ALLA CLASSIFICAZIONE DEI RISCHI – SISTEMI AD ALTO RISCHIO

II. Obblighi dei DEPLOYER

Oltre agli obblighi a carico dei fornitori, anche i **deployer**, cioè gli **utilizzatori dei sistemi di IA**, sono **tenuti** a **rispettare requisiti specifici, per garantire la conformità e la sicurezza dei sistemi di IA ad alto rischio**. Tra gli obblighi principali previsti **dall'articolo 26 dell'AI Act**, i **deployer** devono assicurare i seguenti requisiti:

1. **Documentazione tecnica** I **deployer** devono garantire **l'utilizzo del sistema in conformità con la documentazione tecnica fornita dal fornitore**, seguendo le **istruzioni d'uso** e garantendo che siano rispettate le procedure di sicurezza previste.
2. **Sorveglianza umana** Inoltre, devono affidare la **sorveglianza umana a persone competenti** e adeguatamente **formate**, al fine di garantire il corretto funzionamento e **intervento** in caso di **necessità**.
3. **Monitoraggio post-commercializzazione** È responsabilità dei **deployer** **monitorare l'utilizzo** del **sistema** e **raccogliere dati relativi ai possibili impatti o rischi** derivanti dall'uso della tecnologia. Inoltre, i **deployer** devono **segnalare** eventuali **malfunzionamenti** o **rischi** al **fornitore** e alle autorità competenti, nel caso in cui vengano individuati problemi di sicurezza o violazioni dei diritti fondamentali.
4. **Garanzia di tracciabilità** Così come imposto per i fornitori, i **deployer** sono tenuti a **conservare i log generati dal sistema**, per un periodo di **almeno 6 mesi**, salvo diversa disposizione normativa.

APPLICAZIONE IN BASE ALLA CLASSIFICAZIONE DEI RISCHI - SISTEMI AD ALTO RISCHIO

5. **Obblighi di informazione ai lavoratori** **Prima** di **mettere in servizio** o utilizzare un **sistema di IA ad alto rischio** sul luogo di lavoro, i **deployer** che rivestono il **ruolo di datori di lavoro** devono **informare** i **rappresentanti dei lavoratori e i lavoratori interessati** riguardo **all'uso** del **sistema di IA**, in conformità con lo Statuto dei Lavoratori e normativa applicabile.
6. **Valutazione d'impatto sui diritti fondamentali** È **obbligatorio** per i **deployer** effettuare una **valutazione d'impatto sui diritti fondamentali** per **garantire** che **l'uso del sistema non violi i diritti e le libertà degli individui**, come richiesto dall'art. 27 dell'AI Act.
7. **Obblighi collegati ai dati personali** Inoltre, dovranno effettuare una **valutazione d'impatto** sulla **protezione dei dati**, in conformità con **l'articolo 35 del GDPR**, nel caso in cui il sistema tratti dati personali

In sintesi, sia i **fornitori** che i **deployer** di **sistemi di IA ad alto rischio** **hanno** una **serie di obblighi** importanti per **garantire** la **conformità** alle **normative europee** e la **sicurezza nell'uso** della **tecnologia**

APPLICAZIONE IN BASE ALLA CLASSIFICAZIONE DEI RISCHI – SISTEMI A RISCHIO LIMITATO

C. Sistemi a rischio limitato

- Questi sistemi presentano un **rischio moderato**, ma hanno **potenziali implicazioni per gli utenti**, richiedendo un certo livello di **trasparenza** e **accountability** (responsabilizzazione).

- **non rappresentano una minaccia significativa** per i **diritti fondamentali**, la **sicurezza** o **altri aspetti critici**, ma **richiedono** comunque una **gestione attenta**;
- Gli **utenti** devono essere **informati** che **stanno interagendo** con un **sistema di IA**, in modo da poter prendere **decisioni consapevoli**;
- A differenza dei sistemi ad alto rischio **non sono necessarie valutazioni di conformità approfondite o certificazioni specifiche**.

- Es. uso di Chatbot basato su IA per gestire le richieste dei clienti

APPLICAZIONE IN BASE ALLA CLASSIFICAZIONE DEI RISCHI – SISTEMI A RISCHIO MINIMO

D. Sistemi a rischio minimo

- Tutti gli altri **sistemi di IA non rientranti nelle categorie precedenti**. Non sono soggetti a **obblighi particolari**, ma è **incoraggiata l'adozione** di **codici di condotta volontari.**
- Alcuni esempi:

- **Giochi basati sull'IA**
- **Filtri antispan per mail**
- **Strumenti di raccomandazioni per contenuti non sensibili, come suggerimenti di film e musica**

La classificazione dei sistemi di IA
l'approccio basato sul rischio

Sistemi di IA a rischio inaccettabile

Sistemi di IA ad alto rischio

Sistemi di IA a rischio limitato

Sistemi di IA a rischio basso

CLASSIFICAZIONE SISTEMI DI AI ACT E CONTROLLO AUTORITA' DI VIGILANZA

- I **fornitori** di **sistemi di IA** hanno la **possibilità** di **classificare** il **proprio sistema di AI ACT** come **non ad alto rischio**, **attestandone le caratteristiche e seguendo la procedura di autovalutazione** prevista **dall'art. 43 dell'AI ACT** e dall'allegato VI.
- Laddove **l'Autorità di Vigilanza nazionale** (in Italia dovrebbe essere AgiD) abbia **fondati motivi** di ritenere che i sistemi di AI ACT proposti, **debbano rientrare** tra quelli ad **alto rischio, viene attribuito loro il potere di effettuare valutazioni ulteriori.**

Se confermano i sospetti rientrando **il sistema di AI ad alto rischio, le autorità** chiederanno di **porre in essere senza ritardo le misure necessarie previste dall'AI ACT per i sistemi ad alto rischio.**

La mancata adozione delle misure comporterà l'applicazione di sanzioni ex art. 99 dell'AI ACT, l'adozione di misure provvisorie per vietare o limitare la messa a disposizione del sistema di AI oltre alla notifica alla Commissione e alle autorità di vigilanza di altri stati.

AUTORITA NAZIONALI DI VIGILANZA AI ACT

Chi vigilerà sull'AI Act in Italia?

L'AI Act richiede (art.70) che gli **Stati membri** istituiscano almeno **un'autorità di notifica** e **una di vigilanza del mercato**, con poteri indipendenti e risorse adeguate.

L'«**autorità di notifica**» si occupa di **controllare** e **autorizzare** gli **enti che**, a loro volta, **certificano i sistemi di intelligenza artificiale considerati ad alto rischio.**

L'«**autorità di vigilanza del mercato**» invece **tiene d'occhio i sistemi di AI già in commercio**, assicurandosi che **rispettino le regole stabilite dalle norme europee**. (hanno 24 mesi per conformarsi alle nuove regole)

Ogni paese può decidere come organizzare queste squadre. In **Italia, il disegno di legge n. 1146 del 2024** ha identificato **due enti preposti**:

- **Agenzia per l'Italia Digitale (AgID)**: responsabile della **promozione** e della **conformità** dei **sistemi di IA**.
- **Agenzia per la Cybersicurezza Nazionale (ACN)**: incaricata della **vigilanza**, incluse le **ispezioni** e le **sanzioni**.

➨ **Gli Stati membri** hanno tempo fino al **2 agosto di quest'anno** per **nominare** e **rendere operative le proprie autorità responsabili**. In Italia, oltre ad **AgID** e **ACN**, potrebbe giocare un ruolo importante nei limitare i rischi anche il **Garante per la protezione dei dati personali**, come avvenuto in questi giorni per il caso **DeepSeek** e in passato per **ChatGpt**.

AUTORITA EUROPEA DI VIGILANZA AI ACT

Chi vigilerà sull'AI Act in Europa?

A livello **europeo**, è stato istituito **l'European AI Office**, con compiti di **supporto all'attuazione della normativa** e **monitoraggio** dei modelli di IA per finalità generali.

Il **Comitato europeo per l'intelligenza artificiale**, composto dai **rappresentanti degli Stati membri**, avrà invece il compito di fornire **consulenza** e **coordinare le autorità nazionali**.

SANZIONI


SANZIONI ED ESECUZIONE
Fino al 7% del fatturato annuo globale o 35 milioni di euro per violazioni dell'IA vietate
Fino al 3% del fatturato annuo globale o 15 milioni di euro per la maggior parte delle altre violazioni
Fino all'1,5% del fatturato annuo globale o 7,5 milioni di euro per aver fornito informazioni errate
Tetti alle sanzioni per PMI e startup
Istituiti l'"Ufficio AI" e il "Consiglio AI" europei a livello centrale a livello dell'UE
Autorità di vigilanza del mercato nei paesi dell'UE per applicare la legge sull'AI
Qualsiasi individuo può presentare reclami in caso di non conformità

SCHEMA AI ACT