



AI ACT: CIÒ CHE DEVI (VERAMENTE) SAPERE

11 LUGLIO 2024

ADVANT Nctm

L'AI ACT

INTRODUZIONE

ADVANT Nctm



L'AI ACT

CHE COS'È L'INTELLIGENZA ARTIFICIALE?

L'intelligenza artificiale è una **tecnologia** che rende una macchina in grado di simulare funzioni cognitive umane come la percezione, il pensiero, il ragionamento e l'apprendimento.

I sistemi ai quali questa tecnologia è applicata sono noti come **sistemi di intelligenza artificiale**.

I sistemi di intelligenza artificiale si distinguono da altri sistemi per la loro capacità di inferenza e cioè di ottenere *output* e ricavare modelli e/o algoritmi dai dati/*input* ricevuti.

Per farlo si servono di tecniche di **machine learning** (apprendimento automatico) che consistono nell'addestramento di modelli con set di dati (più o meno grandi).

La tecnica più avanzata di *machine learning* è il **deep learning** (apprendimento profondo) i cui **modelli**, basati su strutture algoritmiche specifiche chiamate reti neurali, sono addestrati con enormi set di dati non strutturati. I *large language models* sono modelli di *deep learning* che consentono al sistema di intelligenza artificiale di rispondere a domande e generare testo. Sono impiegati dai sistemi di intelligenza artificiale generativa, come ChatGPT.

L'AI ACT

PER COSA È E SARÀ UTILIZZATA L'INTELLIGENZA ARTIFICIALE?

L'esperienza quotidiana offre già numerose occasioni di contatto con sistemi di intelligenza artificiale.

Quando effettuiamo una ricerca su Google, traduciamo un testo su DeepL o rivolgiamo una domanda a Siri, i risultati della ricerca, il testo tradotto o il suggerimento di Siri sono tutti *output* generati da sistemi di intelligenza artificiale.

Ma l'ambito di impiego o di possibile impiego dei sistemi di intelligenza artificiale è ben più ampio: dall'industria all'agricoltura, dai trasporti alla salute alle professioni intellettuali, comprese le professioni legali.

L'impatto che, nei prossimi anni, l'intelligenza artificiale potrebbe avere è tale da indurre alcuni a prefigurare l'avvento della **quarta rivoluzione industriale** dopo le macchine a vapore, l'elettricità e l'informatica.

L'AI ACT

QUALI SONO I RISCHI?

L'impiego su vasta scala di sistemi di intelligenza artificiale porta con sé **rischi significativi**.

Per la prima volta nella storia, il lavoro intellettuale potrebbe essere svolto da macchine con la conseguente **scomparsa di talune figure professionali** e ricadute devastanti in termini occupazionali.

C'è poi la questione dell'**imputazione della responsabilità** per i danni cagionati dai sistemi di intelligenza artificiale.

Per non parlare dei rischi di **compressione di libertà e diritti fondamentali** della persona come il diritto a non essere discriminato (sistemi di intelligenza artificiale non programmati correttamente potrebbero assumere decisioni discriminatorie), il diritto alla **protezione dei dati personali** (sistemi di intelligenza artificiale potrebbero raccogliere e trattare illegittimamente dati personali), il **diritto all'informazione** (sistemi di intelligenza artificiale potrebbero diffondere notizie false) e il **diritto alla concorrenza** (nel caso di concentrazione di tecnologie e informazioni in capo a pochi operatori).

L'AI ACT

REGOLARE O NON REGOLARE?

A seconda della prospettiva dalla quale la si guardi, la legge è percepita nel contempo come **garanzia di tutela** e **freno all'innovazione**. Gli stati e le organizzazioni sovranazionali si trovano perciò ora a decidere se regolare o non regolare l'intelligenza artificiale.

La scelta dell'Unione Europea è stata quella di **regolare l'intelligenza artificiale** attraverso un regolamento (quindi direttamente applicabile in tutti gli stati membri).

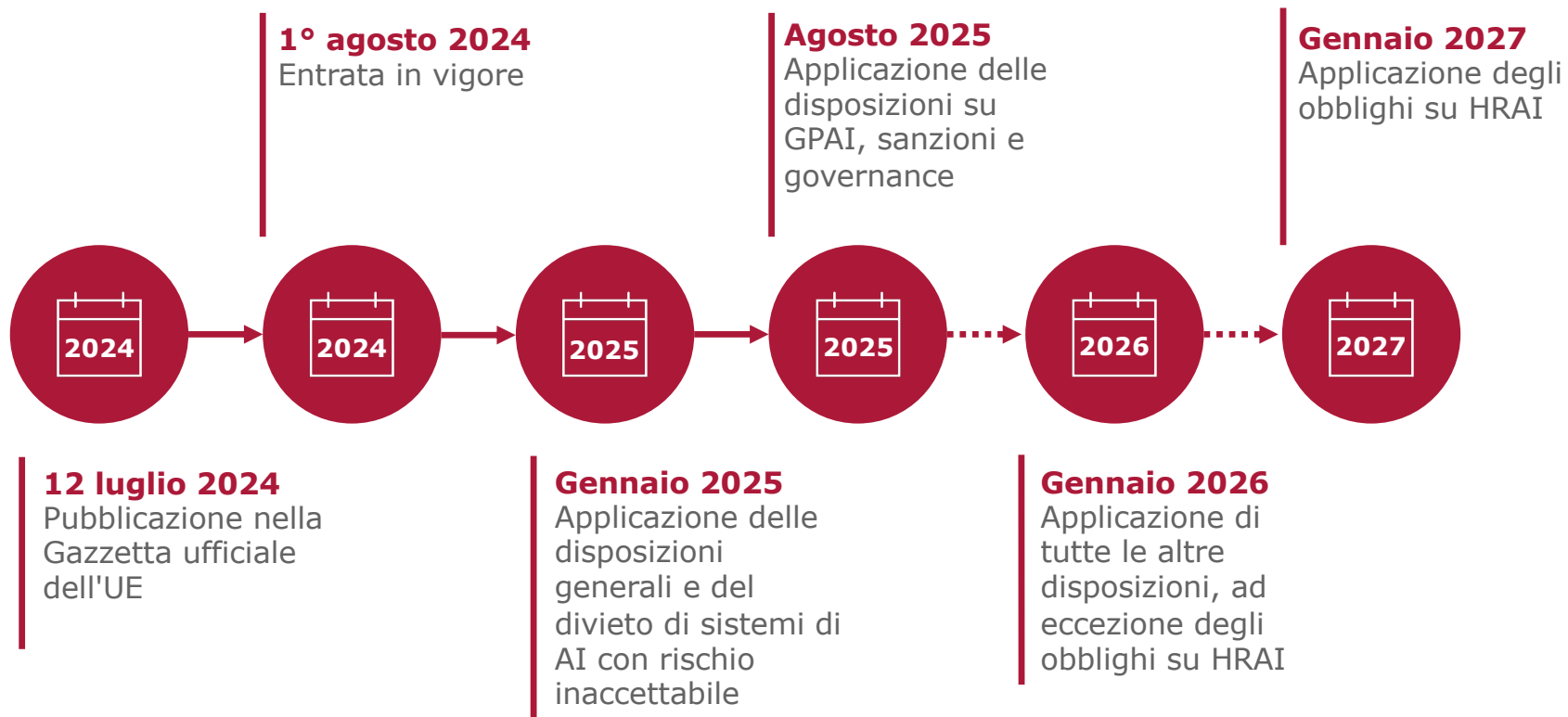
Si tratta del Regolamento UE 2024/1689 più noto come **Artificial Intelligence Act** o AI Act.

L'AI Act è la **prima legge al mondo** che disciplina in maniera organica l'intelligenza artificiale.

Vediamo da quando sarà applicabile.

L'AI ACT

DA QUANDO SI APPLICA?



L'AI ACT

AMBITO DI APPLICAZIONE

ADVANT Nctm



L'AI ACT

A CHI SI APPLICA



L'AI ACT

FORNITORI

Il **fornitore** è la persona fisica o giuridica, l'autorità pubblica, il servizio o l'altro organismo, stabilito nell'Unione o in un paese terzo che sviluppa (o dispone di) un sistema di AI o un modello di AI con finalità generali e che:

- **immette sul mercato** (cioè mette a disposizione per la prima volta sul mercato dell'Unione) il sistema di AI o il modello di AI con finalità generali o;
- **mette in servizio** (cioè rende disponibile al deployer un sistema di AI per essere utilizzato nell'Unione secondo la sua destinazione d'uso) il sistema di AI;
- non immette sul mercato né mette in servizio il sistema di AI ma l'**output prodotto dal sistema è utilizzato nell'Unione**.

L'AI ACT

RAPPRESENTANTI AUTORIZZATI

Il **rappresentante autorizzato** è la persona fisica o giuridica, situata o stabilita nell'UE che ha ricevuto e accettato un **mandato** scritto da un fornitore di sistemi di AI o di modelli di AI con finalità generali non stabilito nell'UE per eseguire e svolgere per suo conto gli obblighi e le procedure stabiliti dal regolamento.

Il mandato deve essere conferito prima della messa a disposizione del sistema nel mercato dell'UE.

Il rappresentante autorizzato deve **recedere** dal mandato nel caso in cui ritenga che il fornitore stia agendo in violazione del regolamento.

Del recesso e delle ragioni del recesso deve essere data comunicazione all'autorità di vigilanza del mercato dello Stato membro in cui è stabilito e, se applicabile, all'organismo notificato.

L'AI ACT

DEPLOYER

Il **deployer** è la persona fisica o giuridica, l'autorità pubblica, il servizio o l'altro organismo che:

- è stabilito nell'Unione e **impiega** un sistema di AI sotto la sua autorità (a meno che il sistema di AI non sia impiegato nell'ambito di attività personali e comunque extra-professionali);
- non è stabilito nell'Unione ma l'**output prodotto dal sistema è utilizzato nell'Unione.**

L'AI ACT

IMPORTATORI E DISTRIBUTORI

L'**importatore** è la persona fisica o giuridica, stabilita nell'Unione, che immette sul mercato un sistema di AI che reca il nome o il marchio di una persona fisica o giuridica stabilita in un paese terzo.

Il **distributore** è qualsiasi persona fisica o giuridica nella catena di fornitura, diversa dal fornitore e dall'importatore, che rende disponibile (cioè fornisce, a titolo oneroso o gratuito, per essere distribuito o utilizzato sul mercato dell'Unione nell'ambito di attività commerciali) un sistema di AI.

L'AI ACT

FABBRICANTI

Il **fabbricante** è la persona fisica o giuridica che fabbrica prodotti integrati con sistemi di AI che:

- **immette sul mercato** o
- **mette in servizio**

con il suo nome o marchio.

L'AI ACT

SISTEMI DI AI E MODELLI DI AI CON
FINALITÀ GENERALI



L'AI ACT

CHE COS'È UN SISTEMA DI AI?

Un sistema di AI è un **sistema che utilizza l'intelligenza artificiale**.

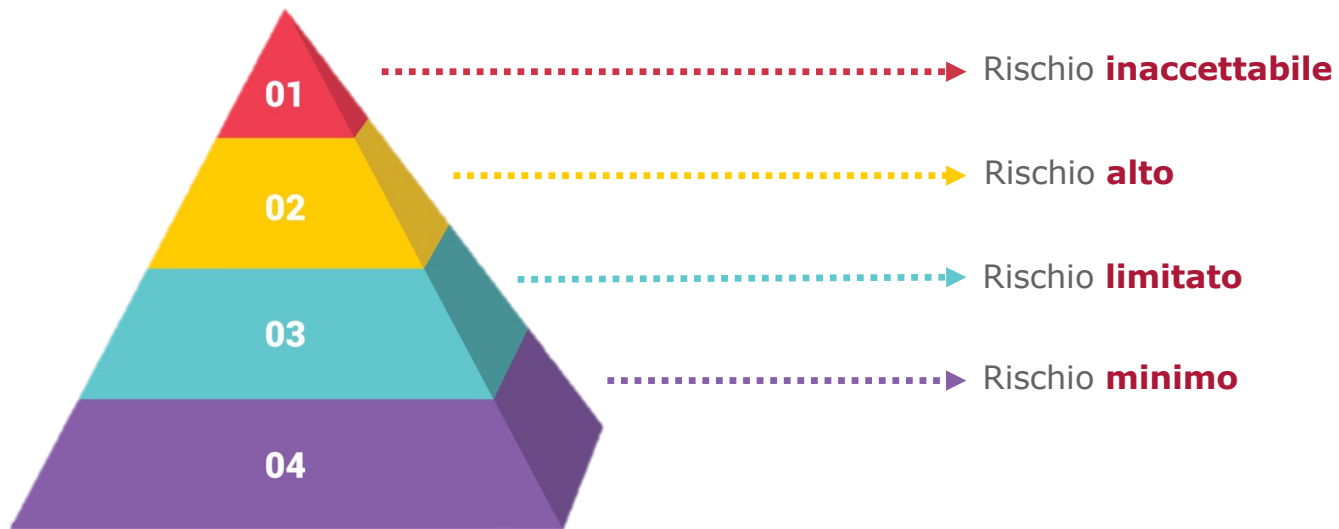
Il regolamento lo definisce come un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, **deduce dall'input che riceve come generare output** quali previsioni, contenuti, raccomandazioni o decisioni **che possono influenzare ambienti fisici o virtuali**.

Non tutti i sistemi di AI sono soggetti ai divieti e alle condizioni imposti dal regolamento ma soltanto quelli che presentano **rischi considerati significativi** dal legislatore europeo.

Sono **quattro** i livelli di rischio.

L'AI ACT

UN APPROCCIO BASATO SUL RISCHIO



L'AI ACT

CHE COS'È UN MODELLO DI AI CON FINALITÀ GENERALI?

Un modello di AI per finalità generali è definito dal regolamento come un modello di AI, anche laddove tale modello di AI sia addestrato con grandi quantità di dati utilizzando l'autosupervisione su larga scala, che sia **caratterizzato da 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, ad eccezione dei modelli di AI utilizzati per attività di ricerca, sviluppo o prototipazione prima di essere immessi sul mercato.

Un esempio di modello di AI per finalità generali è **GPT** (Generative Pre-trained Transformer), sviluppato da OpenAI, che può essere adattato e utilizzato per molteplici scopi senza dover essere ridefinito da zero per ciascuno di essi.

L'AI ACT

SISTEMI DI AI VIETATI

ADVANT Nctm



L'AI ACT

SISTEMI DI AI VIETATI



Sistemi che utilizzano tecniche subliminali, manipolative o ingannevoli



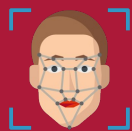
Sistemi che sfruttano vulnerabilità



Sistemi di social scoring



Sistemi di polizia predittiva



Sistemi di riconoscimento facciale basati sullo scraping di immagini facciali



Sistemi di riconoscimento delle emozioni in contesti lavorativi o educativi



Sistemi di categorizzazione biometrica sulla base di dati particolari



Sistemi di identificazione biometrica remota in tempo reale in spazi accessibili al pubblico

L'AI ACT

SISTEMI CHE UTILIZZANO TECNICHE SUBLIMINALI, MANIPOLATIVE O INGANNEVOLI

Possono essere definite **subliminali** le tecniche che mirano a influenzare il comportamento di una persona presentando uno stimolo in modo tale che la persona rimanga inconsapevole dello stimolo presentato.

Le tecniche **manipulative**, invece, perseguono l'obiettivo di cambiare una persona in modo intenzionale e occulto.

L'**inganno**, nel contesto dei sistemi di AI, si riferisce a un atto o a un'omissione intenzionale da parte di un sistema di AI per creare impressioni false o fuorvianti.

I sistemi di AI che utilizzano queste tecniche sono vietati se hanno come obiettivo o come effetto quello di **distorcere in modo significativo il comportamento** di una persona o di un gruppo di persone, compromettendo nella stessa misura la loro capacità di prendere una decisione informata e inducendole così a prendere una **decisione che altrimenti non avrebbero preso**, in un modo che causa o è probabile che causi a quella persona, ad un'altra persona o a un gruppo di persone un **danno significativo**.

L'AI ACT

SISTEMI CHE SFRUTTANO VULNERABILITÀ

Un sistema di AI potrebbe essere progettato per sfruttare le **vulnerabilità** di una persona o di uno specifico gruppo di persone dovute a:

- l'età (ad esempio, minori);
- la disabilità; o
- la situazione sociale o economica (ad esempio, persone che versano in condizioni di estrema povertà).

I sistemi di AI che sfruttano questi tipi di vulnerabilità sono vietati se hanno come obiettivo o come effetto quello di **distorcere in modo significativo il comportamento** di una persona o di una persona appartenente a uno specifico gruppo di persone e determinare un **danno significativo** a carico di queste o altre persone.

L'AI ACT

SISTEMI DI SOCIAL SCORING

I sistemi di *social scoring* sono sistemi di AI per la valutazione o la classificazione di persone o gruppi di persone sulla base del loro **comportamento sociale** o di **caratteristiche note**, desunte o prevedibili relative alla loro persona o alla loro personalità.

Sono vietati i sistemi di *social scoring* che abbiano l'effetto di sottoporre determinate persone o gruppi di persone a un **trattamento pregiudizievole o sfavorevole**:

- in **contesti sociali** che non sono correlati ai contesti in cui i dati sono stati originariamente generati o raccolti;
- che sia **ingiustificato o sproporzionato** rispetto al comportamento sociale tenuto o alla sua gravità.

L'AI ACT

SISTEMI DI POLIZIA PREDITTIVA

I sistemi di polizia predittiva sono sistemi di AI utilizzati per valutare o prevedere il **rischio che una specifica persona commetta un reato**.

I sistemi di polizia predittiva sono vietati se tale valutazione del rischio si basa unicamente sull'analisi de:

- il profilo della **persona**; o
- i tratti e le caratteristiche della sua **personalità**.

Il divieto non si applica solo nel caso in cui siano utilizzati per **avvalorare valutazioni effettuate dall'uomo** che già si basano su fatti oggettivi, verificabili e direttamente collegati ad un'attività criminosa.

L'AI ACT

SISTEMI DI RICONOSCIMENTO FACCIALE BASATI SULLO SCRAPING DI IMMAGINI FACCIALI

Un sistema di AI per la creazione di database di riconoscimento facciale utilizza algoritmi di machine learning per **raccogliere, analizzare e identificare volti nelle immagini** che confluiscono, poi, in database strutturati.

Questo tipo di sistemi di AI fanno spesso uso del c.d. **scraping**, una tecnica che consente al sistema di estrarre automaticamente i dati da pagine web o altre fonti online.

Sono vietati, ai sensi del regolamento, i sistemi di AI che creano o ampliano database di riconoscimento facciale mediante **scraping indiscriminato** (cioè non mirato) di immagini facciali da:

- **Internet**; o da
- filmati di **telecamere** a circuito chiuso.

L'AI ACT

SISTEMI DI RICONOSCIMENTO DELLE EMOZIONI IN CONTESTI LAVORATIVI O EDUCATIVI

I sistemi di riconoscimento delle emozioni **analizzano e interpretano le espressioni facciali** al fine di **identificare le emozioni umane**.

Questi sistemi sono progettati per rilevare e classificare una serie di stati emotivi, come felicità, tristezza, rabbia, sorpresa, disgusto, imbarazzo, eccitazione, vergogna, disprezzo, soddisfazione e divertimento, osservando le caratteristiche del volto umano, come le espressioni degli occhi, della bocca e delle sopracciglia.

Possono essere utilizzati in una varietà di contesti, come il monitoraggio del benessere degli utenti, l'analisi del feedback dei clienti, la personalizzazione dei servizi e l'interazione sociale.

Sono vietati, ai sensi del regolamento, i sistemi di riconoscimento delle emozioni nell'ambito de:

- il **luogo di lavoro**;
- gli **istituti di istruzione**.

Tale divieto non si applica soltanto nel caso in cui tali sistemi siano utilizzati per **motivi medici o di sicurezza**.

L'AI ACT

SISTEMI DI CATEGORIZZAZIONE BIOMETRICA SULLA BASE DI DATI PARTICOLARI

I **dati biometrici** sono i dati relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona (ad esempio, impronte digitali, caratteristiche dell'iride, minute facciali, etc.).

I sistemi di **categorizzazione biometrica** sono quei sistemi che utilizzano i dati biometrici per classificare le persone a cui si riferiscono in categorie.

Sono vietati, ai sensi del regolamento, i sistemi di categorizzazione biometrica che hanno come effetto quello di classificare le persone fisiche in categorie basate su:

- la **razza**;
- le **opinioni politiche**;
- l'**appartenenza sindacale**;
- le **convinzioni religiose o filosofiche**;
- la **vita sessuale o orientamento sessuale**.

Tale divieto non si applica nel caso in cui tali sistemi siano impiegati a fini di contrasto e i dati biometrici siano stati acquisiti in maniera legittima.

L'AI ACT

SISTEMI DI IDENTIFICAZIONE BIOMETRICA REMOTA IN TEMPO REALE IN SPAZI ACCESSIBILI AL PUBBLICO

I sistemi di identificazione biometrica remota in tempo reale in spazi accessibili al pubblico a fini di attività di contrasto sono, di regola, vietati.

Il loro uso è consentito, nella misura in cui ciò sia strettamente necessario e a condizione che siano rispettate le ulteriori condizioni previste dal regolamento (incluso l'ottenimento della preventiva autorizzazione di un'autorità giudiziaria o di un'autorità amministrativa indipendente), per:

- la ricerca mirata di **vittime di sequestri, tratta di esseri umani o sfruttamento sessuale**, nonché per la ricerca di **persone scomparse**;
- la prevenzione di una **minaccia specifica**, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di una minaccia di un **attacco terroristico**;
- la localizzazione o l'identificazione di una **persona sospettata di aver commesso un reato**, nell'ambito di procedimenti penali in relazione a reati puniti con una pena detentiva non inferiore nel massimo a quattro anni.

L'AI ACT

SISTEMI DI AI AD ALTO RISCHIO

ADVANT Nctm



L'AI ACT

QUANDO UN SISTEMA DI AI È AD ALTO RISCHIO?

Un sistema di AI è ad alto rischio se rientra tra i sistemi di AI ad alto rischio elencati nell'**Allegato III** al regolamento o, in ogni caso, se:

- il sistema di AI è destinato a essere utilizzato come componente di sicurezza di un prodotto o è esso stesso un **prodotto soggetto ai regolamenti e alle direttive di cui all'Allegato I** (es. Regolamento Macchine, MDR, IVDR, etc.); e se
- il prodotto, il cui componente di sicurezza è il sistema di AI, o lo stesso sistema di AI 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.

Ricorrendo determinate circostanze, un sistema di AI che pure rientra nell'elenco di cui all'Allegato III, può essere considerato come non ad alto rischio.

La Commissione Europea, mediante atti delegati, può modificare l'elenco dei sistemi di AI ad alto rischio di cui all'Allegato III, stabilire nuove condizioni per la valutazione della rischiosità del sistema nonché fornire orientamenti a beneficio degli operatori.

L'AI ACT

I SISTEMI AD ALTO RISCHIO
DELL'ALLEGATO III

ADVANT Nctm



L'AI ACT

I SISTEMI AD ALTO RISCHIO DI CUI ALL'ALLEGATO III



Sistemi basati sulla biometria



Sistemi nel settore delle infrastrutture critiche



Sistemi nel settore dell'istruzione e della formazione professionale



Sistemi in contesti lavorativi



Sistemi per l'accesso e la fruizione di servizi essenziali



Sistemi a fini di contrasto



Sistemi nel settore della migrazione, dell'asilo e del controllo delle frontiere



Sistemi nel settore dell'amministrazione e della giustizia e dei processi democratici

L'AI ACT

SISTEMI BASATI SULLA BIOMETRIA

Tra i sistemi di AI che si basano sulla biometria, il regolamento considera ad alto rischio i sistemi, diversi da quelli vietati, che rientrano nelle seguenti categorie:

- sistemi di **identificazione biometrica a distanza**, fatta eccezione per quelli il cui solo scopo è di confermare che una determinata persona fisica è la persona che sostiene di essere;
- sistemi destinati ad essere utilizzati per la **categorizzazione biometrica basati sull'inferenza di attributi o caratteristiche sensibili protetti**;
- sistemi di **riconoscimento delle emozioni**.

L'AI ACT

SISTEMI NEL SETTORE DELLE INFRASTRUTTURE CRITICHE

Tra i sistemi di AI impiegati nel settore delle infrastrutture critiche, il regolamento considera ad alto rischio i sistemi di AI destinati ad essere utilizzati quali componenti di sicurezza nella gestione e per il funzionamento di:

- **infrastrutture digitali critiche** (ad esempio, reti di comunicazione elettronica);
- **traffico stradale**;
- fornitura di **acqua, gas, riscaldamento ed elettricità**.

L'AI ACT

SISTEMI NEL SETTORE DELL'ISTRUZIONE E FORMAZIONE PROFESSIONALE

Tra i sistemi di AI impiegati nel settore dell'istruzione e della formazione professionale, il regolamento considera ad alto rischio i sistemi utilizzati per:

- determinare l'**accesso**, l'ammissione o l'assegnazione a istituti di istruzione e formazione professionale;
- valutare i **risultati dell'apprendimento**, anche solo orientando tale processo, negli istituti di istruzione e formazione professionale;
- valutare il **livello di istruzione** appropriato che una persona riceverà o a cui potrà accedere, nel contesto o all'interno di un istituto di istruzione e formazione professionale;
- monitorare e individuare **comportamenti vietati** degli studenti durante le prove nel contesto o all'interno degli istituti di istruzione e formazione professionale.

L'AI ACT

SISTEMI IN CONTESTI LAVORATIVI

Tra i sistemi di AI impiegati in ambito lavorativo, il regolamento considera ad alto rischio i sistemi utilizzati per:

- l'**assunzione** o la **selezione** del personale (in particolare per pubblicare annunci di lavoro mirati, analizzare o filtrare le candidature e valutare i candidati);
- **prendere decisioni** riguardanti le condizioni dei rapporti di lavoro ovvero la promozione o la cessazione dei rapporti contrattuali di lavoro;
- **assegnare compiti** basati sul comportamento individuale o su tratti o caratteristiche personali; e
- **monitorare e valutare le prestazioni** e il comportamento delle persone in tali relazioni.

L'AI ACT

SISTEMI PER L'ACCESSO E LA FRUIZIONE DI SERVIZI ESSENZIALI

Tra i sistemi di AI impiegati per consentire ai cittadini di accedere a e fruire di servizi (privati e pubblici) essenziali, il regolamento considera ad alto rischio i sistemi utilizzati per:

- valutare l'ammissibilità a beneficiare di prestazioni e servizi di **assistenza pubblica** essenziali, compresi i servizi di assistenza sanitaria, nonché concedere, ridurre, revocare o recuperare tali prestazioni e servizi;
- valutare l'**affidabilità creditizia** e stabilire il **merito creditizio** (ad eccezione dei sistemi di AI utilizzati per individuare frodi finanziarie);
- valutare i rischi e determinare i prezzi in caso di assicurazioni sulla vita assicurazioni sanitarie;
- valutare e classificare le **chiamate di emergenza** effettuate per richiedere o inviare servizi di emergenza di primo soccorso o stabilire priorità nell'invio di tali servizi nonché selezionare i pazienti per quanto concerne l'assistenza sanitaria di emergenza.

L'AI ACT

SISTEMI A FINI DI CONTRASTO

Tra i sistemi di AI impiegati a fini di contrasto, il regolamento considera ad alto rischio i sistemi utilizzati:

- per valutare il rischio che una persona diventi **vittima di reati**;
- come **poligrafi** (macchine della verità) e strumenti analoghi;
- per valutare l'**affidabilità delle prove** nel corso di indagini penali;
- valutare il **rischio di reato o di recidiva**;
- per **profilare** persone nel corso dell'accertamento, dell'indagine o del perseguimento di reati.

L'AI ACT

SISTEMI NEL SETTORE DELLA MIGRAZIONE, ASILO E CONTROLLO DELLE FRONTIERE

Tra i sistemi di AI impiegati nel settore della migrazione, dell'asilo e della gestione del controllo delle frontiere, il regolamento considera ad alto rischio i sistemi utilizzati:

- come **poligrafi** (macchine della verità) o strumenti analoghi;
- per valutare un **rischio** (compresi rischi di sicurezza, rischi di migrazione irregolare o rischi per la salute) posto da una persona che intende entrare o è entrata nel territorio di uno Stato membro;
- per assistere le autorità pubbliche competenti nell'**esame** delle domande di asilo, di visto e di permesso di soggiorno e dei relativi reclami per quanto riguarda l'ammissibilità delle persone che richiedono tale status (ivi compresa la valutazione dell'affidabilità delle prove).
- per individuare, riconoscere o **identificare persone** (ad eccezione della verifica dei documenti di viaggio).

L'AI ACT

SISTEMI NEL SETTORE DELL'AMMINISTRAZIONE DELLA GIUSTIZIA E NEI PROCESSI DEMOCRATICI

Tra i sistemi di AI impiegati nei settore dell'amministrazione della giustizia e nei processi democratici, il regolamento considera ad alto rischio i sistemi utilizzati:

- per assistere un'autorità giudiziaria nella **ricerca e nell'interpretazione dei fatti e del diritto** e nell'applicazione del diritto a un insieme di fatti o utilizzati in modo analogo nella risoluzione alternativa delle controversie;
- per influenzare **l'esito di un'elezione o di un referendum o il comportamento di voto** delle persone nell'esercizio del loro voto in elezioni o referendum.

L'AI ACT

REQUISITI DEI SISTEMI AD ALTO
RISCHIO

ADVANT Nctm



L'AI ACT

REQUISITI DEI SISTEMI AD ALTO RISCHIO



**Sistema di gestione
dei rischi**



**Procedure per
garantire la qualità
dei dati**



**Documentazione
tecnica**



**Registrazione dei
log**



Istruzioni d'uso



**Supervisione
umana**



**Accuratezza,
robustezza e
cybersecurity**

L'AI ACT

SISTEMA DI GESTIONE DEI RISCHI

Un sistema di gestione dei rischi è un insieme di processi, procedure e strumenti progettati per **identificare, valutare e gestire**, in maniera continuativa e per l'intero ciclo di vita del sistema di AI ad alto rischio, i **rischi** che gli stessi sistemi pongono **per la salute, la sicurezza e i diritti fondamentali**.

I rischi identificati devono essere gestiti attraverso l'adozione di **misure di gestione del rischio**.

Le misure di gestione del rischio devono consentire di:

- **contenere il rischio residuo** associato a ciascun pericolo (e il rischio residuo complessivo del sistema di AI ad alto rischio) a un livello accettabile;
- garantire, nei limiti in cui ciò sia tecnicamente fattibile, l'**eliminazione o la riduzione dei rischi rilevati** attraverso una progettazione e uno sviluppo del sistema di AI ad alto rischio adeguati;
- ove necessario, garantire **la mitigazione e il monitoraggio dei rischi** che non possono essere eliminati;
- garantire che siano fornite ai deployer le **istruzioni d'uso** e che sia erogata loro la **formazione** eventualmente necessaria.

Ai fini dell'individuazione delle misure di gestione del rischio più appropriate, i sistemi di AI ad alto rischio sono sottoposti a prove, da effettuare prima dell'immissione sul mercato o della messa in servizio.

L'AI ACT

PROCEDURE PER GARANTIRE LA QUALITÀ DEI DATI

I set di dati (personali e non) utilizzati per l'addestramento, la convalida e la prova dei modelli su cui si basano i sistemi di AI ad alto rischio devono essere soggetti a **procedure atte a garantire la qualità dei dati**, che tengano in considerazione in particolare:

- le **scelte progettuali** del caso;
- i **processi di raccolta dei dati** e la loro **fonte** (e, in caso di dati personali, la finalità originaria della raccolta);
- le attività di trattamento per la **preparazione** dei dati (es. etichettatura, pulizia, aggiornamento, etc.);
- la formulazione di **assunzioni**, in particolare per quanto riguarda le informazioni che i dati dovrebbero misurare e rappresentare;
- la **disponibilità**, la **quantità** e l'**adeguatezza** dei set di dati necessari;
- i **possibili errori** che potrebbero pregiudicare la salute e la sicurezza delle persone, incidere negativamente sui diritti fondamentali o portare a discriminazioni vietate dal diritto dell'Unione;
- **misure** idonee a individuare, prevenire e mitigare i possibili errori;
- le modalità per **individuare (e rimediare a) le lacune e le carenze** dei dati che impediscono di raggiungere la piena conformità.

L'AI ACT

DOCUMENTAZIONE TECNICA

La conformità dei sistemi di AI ad alto rischio ai requisiti del regolamento deve essere documentata attraverso la redazione della documentazione tecnica. La documentazione tecnica deve contenere almeno:

- una **descrizione generale del sistema** di AI ad alto rischio;
- una **descrizione dettagliata degli elementi del sistema** di AI ad alto rischio e del processo di sviluppo;
- informazioni di dettaglio sul **monitoraggio, il funzionamento e il controllo** del sistema di AI ad alto rischio;
- una descrizione dell'adeguatezza delle metriche di prestazione per lo specifico sistema di AI ad alto rischio;
- una **descrizione dettagliata del sistema di gestione dei rischi**;
- una descrizione delle **modifiche rilevanti apportate dal fornitore** al sistema di AI ad alto rischio nel corso del suo ciclo di vita;
- l'elenco delle **norme armonizzate applicate** (in tutto o in parte);
- una copia della **dichiarazione di conformità**;
- una descrizione dettagliata del sistema in uso per valutare le **prestazioni del sistema** di AI ad alto rischio nella fase successiva alla commercializzazione.

L'AI ACT

REGISTRAZIONE DEI LOG

I sistemi di AI ad alto rischio devono consentire la **registrazione automatica dei log** per l'intero ciclo di vita del sistema. In particolare, devono essere registrati i log utili a:

- rilevare quelle situazioni da cui possa derivare un rischio o una modifica sostanziale;
- facilitare il monitoraggio post-marketing;
- monitorare il funzionamento del sistema.

I **sistemi di identificazione biometrica da remoto** devono registrare la data e l'ora e la data e l'ora di fine di ogni utilizzo, il database di riferimento rispetto al quale i dati di input sono stati controllati dal sistema, i dati di input per i quali la ricerca ha determinato una corrispondenza e l'identità delle persone fisiche coinvolte nella verifica dei risultati.

L'AI ACT

ISTRUZIONI D'USO

I sistemi di AI ad alto rischio devono essere accompagnati dalle istruzioni d'uso per i deployer. Le istruzioni d'uso devono contenere almeno informazioni circa:

- l'identità e i dati di contatto del **fornitore** e, se applicabile del rappresentante autorizzato;
- le **caratteristiche, potenzialità e limiti di prestazione** del sistema, inclusi la destinazione d'uso, il livello di accuratezza, le circostanze da cui possono derivare rischi, la capacità del sistema di fornire informazioni utili a spiegare i suoi output, le prestazioni in relazione a persone o gruppi di persone a cui il sistema è destinato, informazioni sui set di dati e su addestramento, convalida e testing degli stessi e informazioni per consentire ai deployer di interpretare e utilizzare correttamente gli output;
- le eventuali **modifiche** al sistema di AI ad alto rischio e alle sue prestazioni predeterminate dal fornitore al momento della valutazione iniziale di conformità;
- le misure di **supervisione** umana, comprese quelle per facilitare l'interpretazione degli output da parte dei deployer;
- le **risorse** computazionali e hardware necessarie, **durata** di vita prevista del sistema e misure per la **manutenzione** e la protezione del sistema;
- la descrizione dei meccanismi che consentono ai deployer di raccogliere, archiviare e interpretare correttamente i **log**.

L'AI ACT

SUPERVISIONE UMANA

I sistemi di AI ad alto rischio devono poter essere supervisionati da persone fisiche. I sistemi di AI ad alto rischio devono perciò prevedere **misure di supervisione umana** che mettano il deployer nelle condizioni di:

- comprendere le funzionalità e i limiti del sistema e monitorarne il funzionamento;
- essere consapevoli che il sistema potrebbe indurlo ad affidarsi automaticamente o a fare eccessivo affidamento sui risultati prodotti;
- interpretare correttamente i risultati del sistema;
- decidere, in particolari situazioni, di non utilizzare il sistema o di non tenere conto, ignorare o ribaltare i risultati del sistema;
- intervenire sul funzionamento del sistema o arrestare il sistema attraverso un pulsante di "stop" o una procedura simile.

I **sistemi di identificazione biometrica da remoto** devono prevedere, in aggiunta, misure di supervisione umana atte a far sì che nessuna azione o decisione venga presa dal deployer sulla base dell'identificazione risultante dal sistema, a meno che questa non sia stata verificata e confermata separatamente da almeno due persone fisiche con la necessaria competenza, formazione e autorità.

L'AI ACT

ACCURATEZZA, ROBUSTEZZA E CYBERSECURITY

I sistemi di AI ad alto rischio devono essere progettati e sviluppati per mantenere per tutto il ciclo di vita del sistema un livello adeguato di accuratezza, robustezza e cybersecurity.

Il livello di **accuratezza** deve essere indicato nelle istruzioni d'uso.

Per garantire un livello adeguato di **robustezza**, devono essere adottate misure tecniche (es. backup) che rendano il sistema il più resiliente possibile a eventuali errori, guasti o incongruenze, eliminando o riducendo, nel caso di sistemi che continuano ad apprendere dopo l'immissione in commercio o la messa in servizio, il rischio che i risultati possano condizionare gli input per le operazioni future (c.d. «feedback loop»).

Per garantire un livello adeguato di **cybersecurity**, devono essere adottate misure in grado di prevenire, rilevare e reagire ad attacchi informatici che sfruttano vulnerabilità del sistema (es. data poisoning, model poisoning, adversarial examples, model evasion, etc.).

L'AI ACT

OBBLIGHI DEI FORNITORI

ADVANT Nctm



L'AI ACT

OBBLIGHI DEI FORNITORI



**Conformità ai
requisiti dei
sistemi ad alto
rischio**



Etichettatura



**Sistema di
gestione della
qualità**



**Conservazione
della
documentazione
e tecnica**



**Registrazione
dei log**



**Valutazione di
conformità**



Registrazione



**Ritiro, richiamo
e obblighi di
segnalazione**



**Cooperazione
con le autorità**

L'AI ACT

OBBLIGHI DEI FORNITORI

Il fornitore deve:

- garantire la **conformità del sistema ai requisiti** dei sistemi di AI ad alto rischio (oltre che ai requisiti di accessibilità);
- indicare sul sistema o quantomeno nell'imballaggio o nella documentazione di accompagnamento il suo **nome**, la sua denominazione commerciale o il suo marchio nonché l'**indirizzo** a cui può essere contattato;
- adottare un **sistema di gestione della qualità**;
- conservare per 10 anni la **documentazione relativa al sistema** (documentazione tecnica, dichiarazione di conformità, etc.);
- conservare per almeno 6 mesi i **log** generati automaticamente dal sistema;
- sottoporre il sistema alla procedura di **valutazione della conformità** pertinente, elaborare la **dichiarazione di conformità** e apporre il **marchio CE** sul sistema o quantomeno nell'imballaggio o nella documentazione di accompagnamento;
- registrarsi e registrare il sistema nella **banca dati UE** (nei casi in cui la registrazione sia obbligatoria);
- adottare le **misure correttive necessarie** (compresi ritiro e richiamo) e ottemperare agli obblighi informativi;
- **dimostrare** la conformità del sistema, qualora gli sia richiesto dall'autorità di vigilanza.

ADVANT Nctm

L'AI ACT

SISTEMA DI GESTIONE DELLA QUALITÀ

La funzione del sistema di gestione della qualità è quella di **garantire la conformità** al regolamento. Il sistema di gestione della qualità deve comprendere, tra gli altri:

- una **strategia** per la conformità normativa;
- le **procedure** da seguire nelle fasi di progettazione, sviluppo, esame, prova e convalida;
- i sistemi e le procedure per la **gestione dei dati**;
- il sistema di **gestione dei rischi**;
- il **sistema di monitoraggio** successivo all'immissione sul mercato;
- le procedure relative alla **segnalazione di incidenti** gravi;
- la gestione della **comunicazione** con le autorità nazionali competenti, gli organismi notificati, altri operatori, clienti o altre parti interessate;
- i sistemi e le procedure per la conservazione dei **log** e di tutte le informazioni e la documentazione pertinenti;
- la **gestione delle risorse**, comprese le misure relative alla sicurezza dell'approvvigionamento;
- la definizione di **ruoli e responsabilità** all'interno dell'organizzazione.

L'AI ACT

OBBLIGHI DEI RAPPRESENTANTI
AUTORIZZATI

ADVANT Nctm



L'AI ACT

OBBLIGHI DEI RAPPRESENTANTI AUTORIZZATI

Il rappresentante autorizzato ha l'obbligo di eseguire i compiti indicati nel mandato conferitogli dal fornitore. Il mandato deve attribuire al rappresentante autorizzato il potere di:

- verificare che il fornitore abbia redatto la **dichiarazione di conformità** UE e la **documentazione tecnica** e che abbia effettuato la **valutazione di conformità**;
- conservare (per almeno 10 anni dalla data di immissione in commercio o messa in servizio) e mettere a disposizione delle autorità nazionali competenti i **dati di contatto del fornitore** e una **copia della dichiarazione di conformità** UE, della **documentazione tecnica** e, se applicabile, del **certificato di conformità** rilasciato dall'organismo notificato;
- fornire alle autorità nazionali competenti, su richiesta, le informazioni e i documenti necessari a **dimostrare** la conformità del sistema di AI ad alto rischio all'AI Act (inclusi i log generati automaticamente dal sistema nella disponibilità del fornitore);
- **cooperare** con le autorità competenti in relazione alle decisioni da queste assunte;
- se applicabile, adempiere agli obblighi di **registrazione**.

L'AI ACT

OBBLIGHI DEGLI IMPORTATORI

ADVANT Nctm



L'AI ACT

OBBLIGHI DEGLI IMPORTATORI

L'importatore ha l'obbligo di:

- prima dell'immissione sul mercato, verificare che il fornitore abbia effettuato la **valutazione di conformità**, redatto la **documentazione tecnica** e designato un **rappresentante autorizzato** e che il sistema di AI ad alto rischio rechi il **marchio CE** e sia accompagnato dalla **dichiarazione di conformità** UE e dalle **istruzioni d'uso**;
- **non immettere** sul mercato il sistema di AI ad alto rischio qualora ritenga che esso non sia conforme all'AI Act, informando in caso di rischio il rappresentante autorizzato e l'autorità di vigilanza del mercato;
- indicare sul sistema o quantomeno nell'imballaggio o nella documentazione di accompagnamento il suo **nome**, la sua denominazione commerciale o il suo marchio nonché l'**indirizzo** a cui può essere contattato;
- assicurare che le **condizioni di stoccaggio e trasporto** non compromettano la conformità del sistema di AI ad alto rischio al regolamento;
- conservare (per 10 anni dalla data di immissione in commercio) la **dichiarazione di conformità** UE, le **istruzioni d'uso** e, se applicabile, il **certificato di conformità** rilasciato dall'organismo notificato;
- **fornire** alle autorità nazionali competenti, su richiesta, le informazioni e i documenti necessari a dimostrare la conformità del sistema di AI ad alto rischio al regolamento;
- **cooperare** con le autorità nazionali competenti in relazione alle decisioni da queste assunte.

L'AI ACT

OBBLIGHI DEI DISTRIBUTORI

ADVANT Nctm



L'AI ACT

OBBLIGHI DEI DISTRIBUTORI

Il distributore ha l'obbligo di:

- prima della messa a disposizione sul mercato, verificare che il sistema di AI ad alto rischio rechi il **marchio CE** e sia accompagnato dalla **dichiarazione di conformità** UE e dalle **istruzioni d'uso** e che il fornitore e l'importatore (se presente) abbiano indicato **nome**, denominazione commerciale o marchio e **indirizzo**;
- **non mettere a disposizione** sul mercato il sistema di AI ad alto rischio qualora ritenga che esso non sia conforme all'AI Act, informando in caso di rischio il fornitore e l'importatore (se presente);
- assicurare che le **condizioni di stoccaggio e trasporto** non compromettano la conformità del sistema di AI ad alto rischio all'AI Act;
- qualora ritenga che il sistema di AI ad alto rischio (già messo a disposizione sul mercato) non sia conforme all'AI Act, **intraprendere le azioni correttive necessarie** a rendere conforme il sistema, ritirarlo dal mercato o richiamarlo o comunque garantire che tali azioni correttive siano intraprese dal fornitore o dall'importatore (se presente), informando in caso di rischio il fornitore, l'importatore (se presente) e le autorità nazionali competenti;
- **fornire** alle autorità nazionali competenti, su richiesta, le informazioni e i documenti necessari a dimostrare la conformità del sistema di AI ad alto rischio all'AI Act;
- **cooperare** con le autorità nazionali competenti in relazione alle decisioni da queste assunte.

L'AI ACT

OBBLIGHI DEI DEPLOYER

ADVANT Nctm



L'AI ACT

OBBLIGHI DEI DEPLOYER



**Seguire le
istruzioni per
l'uso**



**Assegnare una
supervisione
umana**



**Dati di input
pertinenti e
rappresentativi**



**Monitoraggio e
segnalazione
degli incidenti**



**Conservazione
dei log**



**Trasparenza
nei confronti
dei lavoratori**



**Trasparenza sui
processi
decisionali
automatizzati**



**Cooperazione
con le autorità**



**Valutazione
d'impatto sui
diritti
fondamentali**

L'AI ACT

OBBLIGHI DEI DEPLOYER

Il deployer ha l'obbligo di:

- adottare misure tecniche e organizzative che assicurino un **utilizzo** del sistema **conforme** alle istruzioni d'uso;
- affidare la sorveglianza umana a persone fisiche in possesso della **competenza**, della **formazione** e dell'**autorità** necessarie e del supporto necessario;
- garantire che i **dati** di input siano **pertinenti e rappresentativi** alla luce della finalità prevista;
- **monitorare** il funzionamento del sistema e **segnalare** al fornitore, all'importatore, al distributore nonché all'autorità nazionale di vigilanza se il sistema presenta un rischio (sospendendo contestualmente l'utilizzo del sistema) nonché ogni incidente grave di cui venga a conoscenza;
- **conservare** per almeno 6 mesi i log generati automaticamente dal sistema;
- **informare i rappresentanti dei lavoratori e i lavoratori** interessati che sono soggette all'uso del sistema di IA ad alto rischio;
- nel caso di sistemi di AI ad alto rischio che adottano decisioni o assistono nell'adozione di decisioni che riguardano persone fisiche, **informare** queste ultime che sono soggette all'uso del sistema di IA ad alto rischio;
- **cooperare** con le autorità nazionali competenti in relazione alle decisioni da queste assunte;
- nel caso di taluni sistemi di AI, effettuare una **valutazione d'impatto sui diritti fondamentali**.

L'AI ACT

VALUTAZIONE D'IMPATTO SUI DIRITTI FONDAMENTALI

L'obbligo di effettuare una valutazione d'impatto sui diritti fondamentali riguarda:

- i deployer di sistemi di AI ad alto rischio che sono **organismi di diritto pubblico o enti privati che forniscono servizi pubblici**;
- i deployer di sistemi di AI per valutare l'**affidabilità creditizia** delle persone fisiche o per stabilire il loro **merito di credito**;
- i deployer di sistemi di AI per la valutazione dei rischi e la determinazione dei prezzi in relazione a persone fisiche nel caso di **assicurazioni sulla vita e assicurazioni sanitarie**.

Nella valutazione, il deployer deve tenere conto, tra le altre cose, dell'ambito di utilizzo del sistema, del tempo e della frequenza di utilizzo, delle categorie di persone fisiche interessate, dei rischi per i diritti fondamentali, delle misure da adottare in caso di concretizzazione dei rischi, etc.

Effettuata la valutazione, il deployer **notifica** i risultati all'autorità di vigilanza.

L'AI ACT

VALUTAZIONE DI CONFORMITÀ,
DICHIARAZIONE DI CONFORMITÀ,
MARCHIO CE E REGISTRAZIONE

ADVANT Nctm



L'AI ACT

CHE COS'È LA VALUTAZIONE DI CONFORMITÀ?

La valutazione di conformità è l'attività che serve a dimostrare la **conformità di un prodotto ai requisiti** stabiliti dalla normativa dell'UE.

Già prevista in relazione a determinate categorie di prodotti, è richiesta dall'AI Act per i **sistemi di AI ad alto rischio**.

Attraverso la valutazione di conformità, è valutata la conformità di un sistema di AI ad alto rischio ai requisiti richiesti dall'AI Act per questo tipo di sistemi (e cioè sistema di gestione del rischio, procedure per garantire la qualità dei dati, documentazione tecnica, registrazione dei log, istruzioni d'uso, sorveglianza umana, accuratezza, robustezza e cybersecurity).

Deve essere effettuata **prima dell'immissione in commercio o della messa in servizio** del sistema di AI ad alto rischio.

Sono previste due procedure per la valutazione di conformità: una **semplificata** e una **ordinaria**.

L'AI ACT

LA VALUTAZIONE DI CONFORMITÀ SEMPLIFICATA

La valutazione di conformità semplificata è quella prevista dall'allegato VI al regolamento.

È richiesta per i sistemi di AI ad alto rischio:

- di cui al punto 1 dell'allegato III (e cioè **sistemi di AI ad alto rischio che si basano sulla biometria**) nel caso in cui il fornitore abbia applicato **norme armonizzate o specifiche comuni**;
- di cui ai punti da 2 a 8 dell'allegato III (e cioè sistemi di AI ad alto rischio nei seguenti settori: **infrastrutture critiche; istruzione e formazione professionale; ambito lavorativo; fini di contrasto; migrazione, asilo e controllo delle frontiere; amministrazione della giustizia e processi democratici**).

La valutazione di conformità semplificata è effettuata dal fornitore **senza il coinvolgimento di un organismo notificato** e si basa su **controlli interni** relativi al sistema di gestione della qualità, alla documentazione tecnica, al processo di progettazione e sviluppo del sistema e al processo di monitoraggio post-marketing.

L'AI ACT

LA VALUTAZIONE DI CONFORMITÀ ORDINARIA

La valutazione di conformità ordinaria è quella prevista dall'allegato VII al regolamento.

È richiesta per i sistemi di AI ad alto rischio di cui al punto 1 dell'allegato III (**sistemi di AI ad alto rischio che si basano sulla biometria**) nel caso in cui:

- **non esistano norme armonizzate** e non siano disponibili specifiche comuni;
- il fornitore **non abbia applicato o abbia applicato solo in parte le norme armonizzate**;
- **le specifiche comuni esistano ma il fornitore non le abbia applicate**;
- una o più norme armonizzate sono state pubblicate con una **limitazione** e solo sulla parte della norma che è stata limitata.

L'AI ACT

LE VALUTAZIONI DI CONFORMITÀ PREVISTE DA ALTRI ATTI UE

Per i **sistemi di AI ad alto rischio soggetti alle direttive e ai regolamenti di cui alla sezione A dell'allegato I** (es. Regolamento Macchine, MDR, IVDR, etc.) la conformità ai requisiti stabiliti dal regolamento è valutata sulla base delle procedure per la valutazione della conformità previste da tali direttive e regolamenti.

Le deroghe dall'obbligo di effettuare una valutazione di conformità previste da tali direttive e regolamenti trovano applicazione unicamente nel caso in cui il fornitore del sistema di AI ad alto rischio abbia applicato le **norme armonizzate** o, se applicabili, le **specifiche comuni**.

L'AI ACT

IL CERTIFICATO DI CONFORMITÀ

Il certificato di conformità è il documento rilasciato dagli **organismi notificati** (coinvolti nella valutazione di conformità ordinaria nonché nelle valutazioni di conformità previste da altri atti UE) che attesta l'esito positivo della valutazione di conformità.

Il certificato deve essere redatto in un linguaggio facilmente comprensibile dalle autorità competenti dello Stato membro in cui è stabilito l'organismo notificato.

La validità del certificato non può essere superiore a **5 anni** per i sistemi di AI ad alto rischio soggetti ad altri atti UE e a **4 anni** per i sistemi di AI ad alto rischio di cui all'allegato III e può essere estesa, rispettivamente, per ulteriori 5 e 4 anni, a seguito di una rivalutazione.

Nel caso in cui ritenga che il sistema di AI ad alto rischio in relazione al quale ha rilasciato un certificato non soddisfi più i requisiti stabiliti dal regolamento, l'organismo notificato può **sospendere o revocare** il certificato nonché imporre restrizioni.

L'AI ACT

LA DICHIARAZIONE DI CONFORMITÀ

La dichiarazione di conformità UE è il **documento con il quale il fornitore dichiara**, assumendosene la responsabilità, **che il sistema di AI ad alto rischio è conforme** ai requisiti stabiliti dal regolamento.

La dichiarazione di conformità UE deve essere redatta in formato leggibile da macchina, essere tradotta nelle lingue degli Stati membri in cui il sistema di AI ad alto rischio è stato immesso sul mercato o reso disponibile, contenere obbligatoriamente le informazioni elencate all'allegato V ed essere sottoscritta dal fornitore.

Deve essere conservata per **10 anni** dalla data dell'immissione sul mercato o della messa in servizio del sistema di AI ad alto rischio ed essere fornita alle autorità nazionali competenti su richiesta.

Per i sistemi di AI ad alto rischio soggetti, oltre che al regolamento, ad altri atti UE che prevedono la dichiarazione di conformità, deve essere redatta un'unica dichiarazione di conformità.

L'AI ACT

IL MARCHIO CE

Sui sistemi di AI ad alto rischio deve essere apposto il **marchio CE**.

In caso di sistemi di AI ad alto rischio in formato digitale deve essere apposto un marchio CE digitale (sempre che il marchio sia facilmente accessibile attraverso l'interfaccia del sistema).

Qualora non sia possibile apporre il marchio CE sul sistema di AI ad alto rischio, questo deve essere apposto sull'**imballaggio** o sulla **documentazione di accompagnamento**.

Se nel corso della procedura di valutazione della conformità è stato coinvolto un organismo notificato, il marchio CE deve essere seguito dal numero identificativo dell'organismo notificato.

L'AI ACT

REGISTRAZIONE

I sistemi di AI ad alto rischio, fatta eccezione per i sistemi di AI ad alto rischio impiegati nel settore delle infrastrutture critiche, devono essere registrati nella **banca dati dell'Unione Europea** dai rispettivi fornitori o rappresentanti autorizzati (che pure devono registrarsi).

Alcune sezioni della banca dati dell'UE sono **sottratte all'accesso** da parte del pubblico. In queste sezioni sono registrati i sistemi di AI ad alto rischio impiegati nei settori delle attività di contrasto, della migrazione, dell'asilo e della gestione del controllo delle frontiere.

I sistemi di AI ad alto rischio impiegati nel settore delle infrastrutture critiche sono registrati in **banche dati nazionali**.

L'AI ACT

OBBLIGHI DI TRASPARENZA PER I
FORNITORI E I DEPLOYER DI
DETERMINATI SISTEMI DI AI



L'AI ACT

SISTEMI DI AI CHE INTERAGISCONO CON PERSONE FISICHE

I fornitori di sistemi di AI destinati a **interagire direttamente con le persone fisiche** devono garantire che il sistema sia progettato e sviluppato in modo tale che le persone fisiche interessate siano **informate** del fatto di stare interagendo con un sistema di AI.

Ciò a meno che il fatto di stare interagendo con un sistema di AI non risulti evidente dal punto di vista di una persona fisica ragionevolmente informata, attenta e avveduta, tenendo conto delle circostanze e del contesto di utilizzo.

Tale obbligo non si applica ai sistemi di AI autorizzati dalla legge per accertare, prevenire, indagare o perseguire reati, fatte salve le tutele adeguate per i diritti e le libertà dei terzi, a meno che tali sistemi non siano a disposizione del pubblico per segnalare un reato.

L'AI ACT

SISTEMI DI AI CHE GENERANO CONTENUTI

I fornitori di sistemi di AI, compresi i sistemi di IA per finalità generali, **che generano contenuti** audio, immagine, video o testuali sintetici, garantiscono che gli output del sistema di IA siano **marcati** in un formato leggibile meccanicamente e rilevabili come generati o manipolati artificialmente.

I fornitori garantiscono che le loro **soluzioni tecniche** siano **efficaci, interoperabili, solide e affidabili** nella misura in cui ciò sia tecnicamente possibile, tenendo conto delle specificità e dei limiti dei vari tipi di contenuti, dei costi di attuazione e dello stato dell'arte generalmente riconosciuto, come eventualmente indicato nelle pertinenti norme tecniche.

Tale obbligo non si applica se i sistemi di AI svolgono una funzione di assistenza per l'editing standard o non modificano in modo sostanziale i dati di input forniti dal deployer o la rispettiva semantica, o se autorizzati dalla legge ad accertare, prevenire, indagare o perseguire reati.

L'AI ACT

SISTEMI DI AI DI RICONOSCIMENTO DELLE EMOZIONI E DI CATEGORIZZAZIONE BIOMETRICA

I deployer di un sistema di riconoscimento delle emozioni o di un sistema di categorizzazione biometrica **informano** le persone fisiche che vi sono esposte in merito al **funzionamento** del sistema e trattano i dati personali in conformità alla normativa in materia di protezione dei dati personali applicabile.

Tale obbligo non si applica ai sistemi di AI utilizzati per la categorizzazione biometrica e il riconoscimento delle emozioni autorizzati dalla legge per accertare, prevenire o indagare reati, fatte salve le tutele adeguate per i diritti e le libertà dei terzi, e conformemente al diritto dell'Unione.

L'AI ACT

SISTEMI DI AI CHE GENERANO DEEP FAKE

Il **deep fake** è un'immagine o un contenuto audio o video generato o manipolato dall'AI che assomiglia a persone, oggetti, luoghi o altre entità o eventi esistenti e che apparirebbe falsamente autentico o veritiero a una persona.

I deployer di un sistema di AI che genera o manipola immagini o contenuti audio o video che costituiscono un deep fake **rendono noto che il contenuto è stato generato o manipolato artificialmente.**

Tale obbligo non si applica se l'uso è autorizzato dalla legge per accertare, prevenire, indagare o perseguire reati.

Qualora il contenuto faccia parte di un'analogia opera o di un programma manifestamente artistici, creativi, satirici o fittizi, gli obblighi di trasparenza di cui al presente paragrafo si limitano all'obbligo di rivelare l'esistenza di tali contenuti generati o manipolati in modo adeguato, senza ostacolare l'esposizione o il godimento dell'opera.

I deployer di un **sistema di AI che genera o manipola testo pubblicato allo scopo di informare il pubblico** su questioni di interesse pubblico rendono noto che il testo è stato generato o manipolato artificialmente.

Tale obbligo non si applica se l'uso è autorizzato dalla legge per accertare, prevenire, indagare o perseguire reati o se il contenuto generato dall'IA è stato **sottoposto a un processo di revisione umana o di controllo editoriale e una persona fisica o giuridica detiene la responsabilità editoriale della pubblicazione del contenuto.**

L'AI ACT

MODELLI DI AI PER FINALITÀ GENERALI

ADVANT Nctm



L'AI ACT

MODELLI DI AI PER FINALITÀ GENERALI E MODELLI DI AI PER FINALITÀ GENERALI CON RISCHIO SISTEMICO

Un modello di AI per finalità generali è classificato come modello di AI per finalità generali con **rischio sistemico** se:

- ha **capacità di impatto elevato** e cioè l'importo cumulativo del calcolo utilizzato per il suo addestramento misurato in FLOP (floating point operations per second) è superiore a 10^{25} ;
- è **classificato come tale dalla Commissione** con sua decisione.

La decisione della Commissione può essere assunta ex officio o all'esito di una procedura che prende avvio con la segnalazione da parte del fornitore del modello per finalità generali della sussistenza del superamento della soglia di cui sopra.

L'AI ACT

OBBLIGHI DEI FORNITORI

Il fornitore di modelli di AI per finalità generali ha l'obbligo di:

- redigere in conformità all'allegato XI (e mantenere aggiornata) la **documentazione tecnica** del modello;
- mettere a disposizione dei fornitori di sistemi di AI che intendono integrare il modello nei loro sistemi di AI le **informazioni** e la **documentazione** necessarie a comprendere le capacità e i limiti del modello e a consentire loro di adempiere agli obblighi a cui sono soggetti e, in ogni caso, le informazioni e la documentazione previste nell'allegato XII;
- definire e attuare **politiche** per adempiere alla normativa dell'Unione in materia di diritto d'autore;
- redigere e mettere a disposizione del pubblico una **sintesi dei contenuti utilizzati per addestrare il modello**;
- **collaborare** con la Commissione e le autorità nazionali competenti.

In aggiunta agli obblighi di cui sopra, il fornitore di modelli di AI per finalità generali con rischio sistemico deve:

- **valutare e attenuare i rischi sistemici** derivanti dallo sviluppo o dall'uso del modello;
- documentare e segnalare all'AI Office e alle autorità nazionali competenti gli **incidenti gravi**;
- garantire un livello adeguato di **cybersecurity**.

L'AI ACT

OBBLIGHI DEI RAPPRESENTANTI AUTORIZZATI

Se è stabilito in un paese terzo, il fornitore di modelli di AI per finalità generali deve nominare un rappresentante autorizzato nell'Unione mediante mandato scritto. Il mandato deve consentire al rappresentante autorizzato di:

- verificare che la **documentazione tecnica** sia stata redatta e che gli **obblighi** a carico del fornitore siano stati adempiuti;
- conservare la documentazione tecnica per **10 anni** dalla data in cui il modello per finalità generali è stato immesso nel mercato dell'Unione;
- mettere a disposizione dell'AI Office e delle autorità nazionali competenti la documentazione tecnica nonché le informazioni e la documentazione necessarie a **dimostrare la conformità** al regolamento;
- **cooperare** con l'AI Office e con le autorità nazionali competenti in relazione alle azioni intraprese da questi ultimi con riguardo ai modelli per finalità generali con rischio sistemico (anche nel caso in cui tali modelli siano integrati in sistemi di AI immessi sul mercato e messi in servizio nell'Unione).

L'AI ACT

MISURE A SOSTEGNO
DELL'INNOVAZIONE

ADVANT Nctm



L'AI ACT

GLI SPAZI DI SPERIMENTAZIONE NORMATIVA

Ciascuno Stato membro deve istituire almeno uno **spazio di sperimentazione normativa**.

Lo spazio di sperimentazione normativa è un **ambiente controllato** in cui i sistemi di AI possono essere sviluppati, addestrati, sperimentati e convalidati sulla base di un piano concordato tra il fornitore del sistema di AI (o il potenziale fornitore di sistemi di AI) e l'autorità competente.

L'autorità competente rilascia al fornitore, su richiesta, una **prova scritta** delle attività svolte con successo e una relazione di uscita che illustra nel dettaglio le attività svolte e i risultati conseguiti.

La prova scritta e la relazione di uscita possono essere utilizzate dal fornitore di sistemi di AI nell'ambito delle procedure per la valutazione della conformità.

L'AI ACT

PROVE IN CONDIZIONI REALI FUORI DAGLI SPAZI DI SPERIMENTAZIONE NORMATIVA

Per poter effettuare **prove in condizioni reali**, il fornitore di sistemi di AI ad alto rischio deve:

- elaborare un **piano di prova** in condizioni reali e sottoporlo all'autorità di vigilanza dello Stato membro in cui devono essere svolte le prove per approvazione;
- **registrare** la prova nella parte non pubblica della banca dati dell'Unione;
- essere **stabilito** nell'Unione o aver nominato un **rappresentante autorizzato** nell'Unione;
- **non trasferire in paesi terzi** i dati raccolti ed elaborati nel corso delle prove, se non in conformità al diritto dell'Unione;
- effettuare le **prove** per il periodo strettamente necessario e, comunque, per non più di 6 mesi, prorogabili di ulteriori 6;
- ottenere il **consenso informato** delle persone coinvolte e assicurare adeguata protezione alle persone vulnerabili;
- concludere con il potenziale deployer coinvolto un accordo per definire le rispettive **responsabilità**;
- supervisionare le prove tramite **personale qualificato**;
- garantire che le previsioni, le raccomandazioni e le decisioni del sistema di AI possano essere **ignorate e ribaltate**.

ADVANT Nctm

L'AI ACT

GOVERNANCE

ADVANT Nctm



L'AI ACT

AI OFFICE

Lo European Artificial Intelligence Office (o, come è più noto, l'**AI Office**) è stato istituito dalla Commissione Europea con provvedimento del 24 gennaio 2024 (la cui efficacia è stata differita al 24 febbraio 2024).

L'AI Office fa parte della Direzione generale delle Reti di comunicazione, dei contenuti e delle tecnologie (CNECT).

All'AI Office è stato assegnato, in particolare, il **controllo dei modelli per finalità generali**. Nell'ambito di questa attività, l'AI Office:

- individua le metodologie e i parametri di riferimento per valutare la capacità dei modelli per finalità generali;
- monitora l'applicazione delle norme relative ai modelli per finalità generali e ai sistemi che ne fanno uso e investiga eventuali violazioni;
- rileva eventuali rischi non prevedibili in relazione all'uso dei modelli per finalità generali.

Svolge, poi, **funzioni di supporto** alla Commissione per contribuire all'efficace attuazione e all'applicazione uniforme del regolamento.

L'AI ACT

EUROPEAN ARTIFICIAL INTELLIGENCE BOARD

Lo **European Artificial Intelligence Board** è composto da un rappresentante per Stato membro. Partecipano alle sue riunioni, senza diritto di voto, anche il Garante Europeo della protezione dei dati e l'AI Office.

Al suo interno, sono istituiti due sottogruppi permanenti di cui uno dedicato a **favorire la cooperazione e lo scambio di informazioni tra le autorità nazionali di vigilanza sul mercato.**

Ha il compito, tra l'altro, di:

- contribuire al **coordinamento** delle autorità nazionali competenti;
- **condividere** conoscenza e *best practice*;
- fornire **consulenza**;
- contribuire all'**armonizzazione delle pratiche amministrative**;
- formulare **raccomandazioni e pareri.**

L'AI ACT

FORUM CONSULTIVO

Il **Forum Consultivo** è istituito dalla Commissione ed è composto da rappresentanti delle principali categorie di *stakeholder* nel settore dell'intelligenza artificiale: industria, start-up, PMI, società civile e mondo accademico.

Ha il compito di:

- redigere **opinioni, raccomandazioni e altri contributi scritti** su richiesta dell'AI Board o della Commissione;
- istituire sottogruppi temporanei al fine di esaminare **specifici quesiti**;
- preparare un **report annuale**, pubblicamente accessibile, sulle attività svolte.

L'AI ACT

GRUPPO DI ESPERTI SCIENTIFICI INDIPENDENTI

Il **Gruppo di esperti scientifici indipendenti** è istituito dalla Commissione ed è composto da esperti in possesso di competenze scientifiche o tecniche nel settore dell'intelligenza artificiale e che siano indipendenti da qualsiasi fornitore di sistemi di AI o di modelli di AI per finalità generali.

Fornisce **supporto all'AI Office** nello svolgimento dei suoi compiti.

Anche gli Stati membri possono avvalersi del supporto del Gruppo di esperti indipendenti.

L'AI ACT

AUTORITÀ NAZIONALI COMPETENTI

Ciascuno Stato Membro istituisce o designa:

- un'**autorità notificante**; e
- un'**autorità di vigilanza sul mercato**.

L'autorità notificante è l'autorità nazionale responsabile dell'istituzione e dell'esecuzione delle procedure necessarie per la valutazione, la designazione e la notifica degli organismi di valutazione della conformità e per il loro monitoraggio.

L'autorità di vigilanza del mercato è l'autorità responsabile della vigilanza del mercato nel territorio dello Stato membro.

L'AI ACT

DATABASE UE DEI SISTEMI DI AI AD
ALTO RISCHIO

ADVANT Nctm



L'AI ACT

DATABASE UE DEI SISTEMI DI AI AD ALTO RISCHIO

La Commissione, in collaborazione con gli Stati Membri, istituisce e mantiene un **database dell'UE** per i sistemi di AI ad alto rischio, il quale contiene le informazioni che l'Allegato VIII richiede di inserire ai fornitori e agli utenti di tali sistemi.

Per lo sviluppo e l'aggiornamento delle **funzionalità tecniche** del database dovranno essere consultati *esperti di settore*.

Le informazioni contenute nel database dovranno essere **pubblicamente accessibili** (salvo specifiche eccezioni) in maniera *user-friendly* con informazioni leggibili dalle macchine.

I dati personali eventualmente contenuti nel database europeo sono raccolti e trattati nella misura in cui sia strettamente necessario (ad es., nomi e dati di contatto delle persone responsabili della registrazione).

La **Commissione** è stata individuata come:

- *titolare del trattamento* dei dati inerenti al database;
- incaricata di garantire *supporto tecnico e amministrativo* ai fornitori e utenti.

L'AI ACT

MONITORAGGIO POST MARKETING,
NOTIFICA DI INCIDENTI E VIGILANZA
DEL MERCATO

ADVANT Nctm



L'AI ACT

SISTEMA DI MONITORAGGIO POST MARKETING

I fornitori di sistemi di AI ad alto rischio devono istituire un **sistema di monitoraggio** post marketing.

Attraverso il sistema di monitoraggio post marketing sono raccolti e analizzati i **dati relativi alle prestazioni** dei sistemi di AI ad alto rischio per tutto il loro ciclo di vita. Ciò al fine di **valutare nel tempo la conformità** dei sistemi di AI ad alto rischio ai requisiti stabiliti dal regolamento.

Il sistema di monitoraggio post marketing si basa su un **piano di monitoraggio** definito alla stregua del modello di piano di monitoraggio adottato dalla Commissione con proprio provvedimento.

Per i sistemi di AI ad alto rischio soggetti alle direttive e ai regolamenti di cui alla sezione A dell'allegato I (es. Regolamento Macchine, MDR, IVDR, etc.), qualora tali direttive e regolamenti già prevedano un sistema e un piano di monitoraggio, i fornitori possono integrare i sistemi e i piani di monitoraggio esistenti con gli elementi ulteriori previsti dall'AI Act (e dal modello di piano di monitoraggio adottato dalla Commissione Europea).

L'AI ACT

NOTIFICA DI INCIDENTI GRAVI

I fornitori di sistemi di AI ad alto rischio devono **notificare qualsiasi incidente grave** all'autorità di vigilanza dello Stato membro in cui l'incidente si è verificato ogniqualvolta esso sia causato da un sistema di AI ad alto rischio o comunque ogniqualvolta il nesso causale sia ragionevolmente probabile.

Per incidente grave si intende l'incidente o il malfunzionamento di un sistema di AI che, direttamente o indirettamente, causa:

- il **decesso** di una persona o gravi danni alla salute di una persona;
- una **perturbazione** grave e irreversibile della gestione o del funzionamento di infrastrutture critiche;
- la **violazione** degli obblighi previsti dal diritto dell'Unione a protezione dei diritti fondamentali;
- gravi **danni** alle cose o all'ambiente.

L'AI ACT

TERMINI PER LA SEGNALAZIONE

La notifica deve essere effettuata immediatamente e comunque non oltre **15 giorni** dal momento in cui il fornitore o il deployer ne è venuto a conoscenza. Il termine di 15 giorni si riduce a:

- **2 giorni** nel caso in cui l'incidente grave abbia causato una perturbazione grave e irreversibile della gestione o del funzionamento di infrastrutture critiche;
- **10 giorni** nel caso in cui l'incidente grave abbia causato il decesso di una persona.

Qualora non si disponga di informazioni complete entro il termine, la notifica può essere completata con le informazioni mancanti anche oltre il termine.

L'AI ACT

ATTIVITÀ SUCCESSIVE ALLA NOTIFICA

Successivamente alla notifica, il fornitore:

- svolge le **indagini** necessarie;
- **coopera** con l'autorità di vigilanza;
- adotta **misure correttive**;
- si astiene dall'apportare al sistema di AI ad alto rischio **modifiche** che impediscano o compromettano la valutazione delle cause dell'incidente senza aver prima informato di ciò l'autorità di vigilanza.

L'autorità di vigilanza:

- nel caso in cui l'incidente abbia causato la violazione degli obblighi previsti dal diritto dell'Unione a protezione dei diritti fondamentali, **informa** le autorità o gli organismi pubblici nazionali a cui è affidata la vigilanza sul rispetto di tali obblighi;
- entro 7 giorni dal ricevimento della notifica, **adotta** le misure appropriate di cui all'art. 19 del Regolamento UE 2019/1020 (Regolamento sulla vigilanza del mercato e sulla conformità dei prodotti).

L'AI ACT

VIGILANZA DEL MERCATO

Quando un'autorità di vigilanza del mercato ha ragioni sufficienti per ritenere che un sistema di AI possa rappresentare un **rischio**, effettua una valutazione della sua conformità al regolamento.

Se la valutazione rivela che il sistema di AI non è conforme ai requisiti stabiliti nel regolamento, l'autorità di vigilanza richiede all'operatore di adottare misure correttive entro un periodo specificato.

Queste misure correttive possono includere:

- la **messa in conformità** del sistema di AI;
- il **ritiro** dal mercato; o
- il **richiamo** del sistema.

Se l'operatore A non adotta misure correttive adeguate nel periodo richiesto, l'autorità di vigilanza del mercato adotta tutte le misure provvisorie del caso per vietare o limitare la messa a disposizione o la messa in servizio del sistema di AI sul mercato nazionale, per ritirare il sistema di AI dal mercato o per richiamarlo.

L'AI ACT

MEZZI DI RICORSO

Fatti salvi altri ricorsi amministrativi o giurisdizionali, qualsiasi persona fisica o giuridica che abbia motivo di ritenere che vi sia stata una violazione delle disposizioni del regolamento può **presentare un reclamo** motivato alla pertinente autorità di vigilanza del mercato.

Qualsiasi persona interessata oggetto di una decisione adottata dal deployer sulla base dell'output di un sistema di AI ad alto rischio elencato nell'allegato III, ad eccezione dei sistemi di AI impiegati nel settore delle infrastrutture critiche, e che produca effetti giuridici o in modo analogo incida significativamente su tale persona in un modo che essa ritenga avere un **impatto negativo sulla sua salute, sulla sua sicurezza o sui suoi diritti fondamentali** ha il diritto di **ottenere dal deployer spiegazioni chiare e significative** sul ruolo del sistema di AI nella procedura decisionale e sui principali elementi della decisione adottata.

L'AI ACT

CODICI DI CONDOTTA E ORIENTAMENTI

ADVANT Nctm



L'AI ACT

CODICI DI CONDOTTA

L'AI Office e gli Stati membri promuovono e agevolano l'elaborazione di **codici di condotta volontaria** in relazione ai sistemi di AI diversi da quelli ad alto rischio, al fine di applicare a questi sistemi alcuni o tutti i requisiti specificati per i sistemi di AI ad alto rischio.

I codici di condotta possono includere **obiettivi chiari** e **indicatori chiave di prestazione** tra cui:

- rispetto degli orientamenti etici dell'Unione per un'AI affidabile;
- riduzione dell'impatto ambientale dei sistemi di AI;
- promozione dell'alfabetizzazione in materia di AI;
- progettazione inclusiva e diversificata dei sistemi di AI;
- valutazione e prevenzione dell'impatto negativo dei sistemi di AI sulle persone vulnerabili.

I codici di condotta possono essere sviluppati da singoli **fornitori, deployer o organizzazioni rappresentative**, coinvolgendo *deployer* e altre parti interessate, come le PMI, le start-up, la società civile e il mondo accademico.

L'AI ACT

ORIENTAMENTI

La Commissione elabora **orientamenti** pratici per l'attuazione del regolamento in relazione ad aspetti quali:

- l'applicazione dei requisiti e degli obblighi previsti dal regolamento;
- le pratiche vietate;
- l'attuazione delle disposizioni relative alla modifica sostanziale;
- l'attuazione pratica degli obblighi di trasparenza;
- la relazione tra il regolamento e altre normative dell'Unione;
- l'applicazione della definizione di sistema di AI.

La Commissione provvede ad **aggiornare** gli orientamenti su richiesta degli Stati membri, dell'ufficio per l'AI o iniziativa propria, quando lo ritiene necessario.

L'AI ACT

DELEGA DI POTERE E PROCEDURA DI
COMITATO

ADVANT Nctm



L'AI ACT

DELEGA DI POTERE E PROCEDURA DI COMITATO

Il regolamento attribuisce alla Commissione il potere di adottare **atti delegati** in relazione a specifici aspetti individuati dal regolamento stesso.

La delega ha una durata di **5 anni** (tacitamente rinnovabili) dalla data di entrata in vigore del regolamento e può essere revocata in qualsiasi momento dal Parlamento europeo e dal Consiglio.

La Commissione:

- prima dell'adozione di un atto delegato, **consulta** gli esperti designati da ciascuno Stato membro;
- contestualmente alla sua adozione, **dà comunicazione** dell'atto delegato adottato al Parlamento europeo e al Consiglio.

Se il Parlamento europeo e il Consiglio non sollevano obiezioni entro tre mesi dalla notifica o se comunicano alla Commissione di non voler sollevare obiezioni, l'atto delegato entra in vigore.

Nella sua attività legislativa regolamentare, la Commissione fa ricorso alla procedura di comitato. Si tratta di un meccanismo che consente il coinvolgimento degli Stati membri nell'elaborazione degli atti delegati alla Commissione.

L'AI ACT

SANZIONI

ADVANT Nctm



L'AI ACT

NATURA ED ENTITÀ DELLE SANZIONI

Sono gli Stati membri a dover stabilire le regole relative alle sanzioni e alle altre misure di esecuzione.

Queste possono includere, secondo il regolamento:

- semplici **avvertimenti**; o
- **sanzioni amministrative pecuniarie.**

Le sanzioni devono essere effettive, proporzionate e dissuasive e tenere conto della sostenibilità economica delle PMI, incluse le start-up.

Sono inflitte dalle autorità nazionali di vigilanza del mercato.

Il regolamento fissa il massimo legale delle sanzioni amministrative pecuniarie applicabili, distinguendo a seconda che la violazione sia stata commessa da:

- **operatori** di sistemi di AI (e cioè fornitori, rappresentanti autorizzati, importatori, distributori e deployer);
- fornitori e rappresentanti autorizzati di **modelli per finalità generali**;
- **istituzioni e organismi dell'Unione.**

L'AI ACT

OPERATORI DI SISTEMI AI

Entità	Violazioni
Fino a €35 milioni o, se impresa, al 7% del fatturato totale mondiale annuo relativo all'esercizio precedente, se superiore	Immissione sul mercato o messa in servizio di sistemi di AI vietati
Fino a €15 milioni o, se impresa, al 3% del fatturato totale mondiale annuo relativo all'esercizio precedente, se superiore	Violazione degli obblighi relativi ai sistemi di AI ad alto rischio e degli obblighi di trasparenza relativi ai sistemi di AI a rischio limitato
Fino a €7.5 milioni o, se impresa, al 1% del fatturato totale mondiale annuo relativo all'esercizio precedente, se superiore	Fornitura di informazioni inesatte, incomplete o fuorvianti agli organismi notificati o alle autorità nazionali competenti

L'AI ACT

FORNITORI DI SISTEMI AI PER FINALITÀ GENERALI

Entità	Violazioni
Fino a €15 milioni o, se impresa, al 3% del fatturato totale mondiale annuo relativo all'esercizio precedente, se superiore	Violazioni delle disposizioni relative ai modelli di AI per finalità generali

L'AI ACT

ISTITUZIONI, ORGANI E ORGANISMI DELL'UNIONE

Entità	Violazioni
Fino a €1.5 milioni	Immissione sul mercato o messa in servizio di sistemi di AI vietati
Fino a €750 mila	Violazione di altri obblighi

L'AI ACT

CRITERI DI COMMISURAZIONE

Per determinare l'importo della sanzione amministrativa pecuniaria si tiene conto de:

- la **natura, gravità e durata** della violazione e delle sue conseguenze;
- le **precedenti sanzioni** applicate da altre autorità di vigilanza nei confronti dello stesso operatore in relazione alla medesima violazione;
- le **precedenti sanzioni** applicate per violazioni di altre normative UE per violazioni derivanti dalla stessa attività/omissione;
- le **dimensioni**, il **fatturato** annuo e la **quota di mercato** dell'operatore;
- altri fattori **aggravanti** o **attenuanti** (ad esempio, i benefici finanziari conseguiti o le perdite evitate);
- il grado di **cooperazione** con l'autorità di vigilanza;
- il grado di **responsabilità** dell'operatore, tenendo conto delle misure tecniche e organizzative attuate;
- il modo in cui l'autorità è venuta a **conoscenza** della violazione;
- il carattere **doloso o colposo** della violazione;
- le **azioni intraprese** per attenuare il danno.

ADVANT Nctm

BEIJING | BERLIN | BRUSSELS | DUSSELDORF | FRANKFURT | HAMBURG
LONDON | MILAN | MOSCOW | MUNICH | PARIS | ROME | SHANGHAI

ADVANT-NCTM.COM