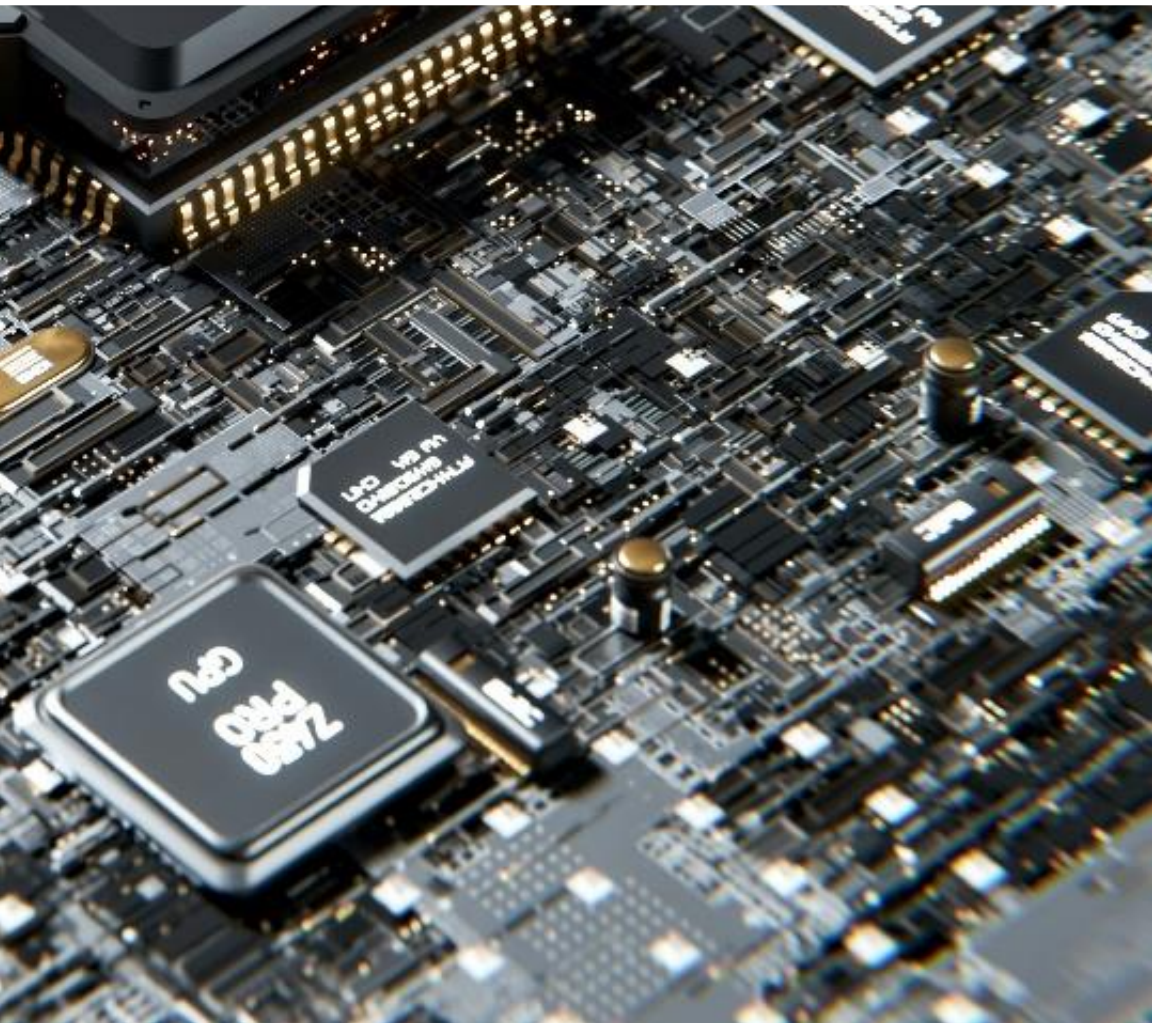
AI Act pronto all'uso: come rendere il tuo Sistema conforme oggi

Strumenti Pratici e domande da porsi per adeguare la tua Azienda alle Nuove Normative sull'Intelligenza Artificiale

A cura di **Alessandro Vestito**

Ottobre 2024



Introduzione

Il contesto dell'AI Act: Una panoramica

Negli ultimi decenni, l'intelligenza artificiale (IA) è emersa come una delle tecnologie più trasformative del nostro tempo. Dalla medicina alla finanza, dall'industria manifatturiera ai servizi digitali, l'IA sta influenzando ogni aspetto della società. Tuttavia, il suo potere dirompente solleva importanti interrogativi etici, legali e sociali. L'Unione Europea ha riconosciuto questa necessità e ha intrapreso un'azione proattiva con l'AI Act, una legislazione innovativa che mira a regolamentare lo sviluppo, la distribuzione e l'uso dell'IA.

L'AI Act rappresenta il primo tentativo su scala globale di disciplinare l'uso dell'intelligenza artificiale, ponendosi come modello per altre giurisdizioni. La normativa mira a creare un quadro giuridico che bilanci l'innovazione con la protezione dei diritti fondamentali, come la privacy e la sicurezza. In questo contesto, la conformità all'AI Act diventa una priorità fondamentale per le organizzazioni che operano con sistemi di intelligenza artificiale nell'Unione Europea o che intendono entrare in questo mercato.

Questa guida alla compliance con l'AI Act si propone di fornire una risorsa pratica e completa per le aziende e i professionisti, al fine di comprendere e implementare le regole stabilite dal regolamento. L'obiettivo è aiutare a navigare le complessità della legislazione, fornendo consigli operativi e best practices per evitare rischi legali e promuovere un uso responsabile dell'IA.

Perché è necessaria una guida alla compliance per l'AI Act?

L'AI Act introduce una serie di obblighi e requisiti che variano a seconda del livello di rischio del sistema IA utilizzato, categorizzati in tre principali livelli: *sistemi ad alto rischio, sistemi a rischio limitato e sistemi a rischio minimo o nullo.* Ogni livello comporta specifiche responsabilità per le imprese e gli sviluppatori, che devono adeguarsi a standard tecnici, requisiti di trasparenza e controlli di sicurezza. In molti casi, tali requisiti possono risultare complessi e richiedere un approccio sistematico per garantire la piena conformità.

Le sanzioni per la mancata compliance non sono irrilevanti. L'AI Act prevede multe significative, che possono arrivare fino al 7% del fatturato globale annuale di un'azienda. È chiaro, quindi, che la conformità non è un'opzione, ma una necessità strategica per evitare impatti finanziari e reputazionali negativi.

Inoltre, la compliance non riguarda solo l'evitare le sanzioni, ma rappresenta un'opportunità per le imprese di dimostrarsi all'avanguardia nell'adozione di pratiche etiche e sostenibili. In un mondo sempre più focalizzato sulla responsabilità sociale e sull'uso consapevole della tecnologia, le aziende che aderiscono alle normative possono costruire fiducia con i loro clienti, investitori e altri stakeholder.

Obiettivi della guida

Questa guida ha l'obiettivo di fornire un supporto pratico per comprendere e applicare le norme previste dall'AI Act. È rivolta a una vasta gamma di lettori, inclusi dirigenti d'azienda, responsabili legali, ingegneri di IA, specialisti in compliance e chiunque abbia responsabilità nella gestione e nello sviluppo di sistemi di intelligenza artificiale.

Gli obiettivi principali di questa guida sono:

- Fornire chiarezza sui requisiti legali: Spiegare in modo semplice e diretto cosa richiede l'AI Act e come si applica ai diversi tipi di sistemi IA.
- Guidare il processo di valutazione del rischio: Aiutare le organizzazioni a classificare i loro sistemi IA in base al livello di rischio e determinare i requisiti specifici di compliance.
- Offrire strumenti operativi per la compliance: Presentare modelli, checklist e suggerimenti pratici per integrare la conformità nei processi aziendali, dalla progettazione iniziale all'implementazione e alla manutenzione dei sistemi IA.
- Promuovere un approccio etico e responsabile: Oltre alla conformità legale, la guida incoraggia le organizzazioni a considerare le implicazioni etiche dell'IA, assicurando che i sistemi rispettino i diritti umani e i valori fondamentali dell'UE.

L'AI Act: Struttura e Principi Fondamentali

Prima di addentrarci nei dettagli pratici della compliance, è importante comprendere i principi su cui si fonda l'AI Act. La legislazione europea si basa su una visione dell'intelligenza artificiale come tecnologia che può contribuire al progresso economico e sociale, ma solo se sviluppata e utilizzata in modo sicuro, trasparente e responsabile. Alcuni dei principi chiave dell'AI Act includono:

- Proporzionalità: Le regole e i requisiti di compliance sono proporzionati al livello di rischio che il sistema IA presenta. Questo significa che non tutte le IA sono soggette agli stessi controlli, evitando così un approccio eccessivamente restrittivo per tecnologie a basso rischio.
- Approccio basato sul rischio: Il cuore dell'AI Act è la valutazione del rischio. I sistemi IA ad alto rischio, come quelli utilizzati nella salute, nella sicurezza pubblica o nella giustizia, sono soggetti a norme più rigorose rispetto a quelli a basso rischio.
- Trasparenza: Le organizzazioni devono garantire che i loro sistemi IA siano trasparenti per gli utenti. Questo include la necessità di fornire informazioni chiare su come funziona il sistema, quali dati utilizza e quali decisioni vengono prese in modo automatizzato.
- Responsabilità e supervisione umana: L'AI Act insiste sulla necessità di mantenere un controllo umano significativo sui sistemi IA, in modo che le decisioni critiche non siano lasciate esclusivamente a macchine.

Il percorso verso la conformità

Per le aziende e i professionisti, la compliance all'AI Act non è un processo che può essere affrontato una sola volta, ma richiede un impegno continuo, anche per mantenersi in regola in seguito all'aggiornamento dei software e ambienti fisici. Dal momento in cui un sistema IA è progettato, fino alla sua implementazione e oltre, devono essere stabiliti meccanismi per garantire il rispetto delle normative. Questo richiede uno sforzo interdisciplinare che coinvolge ingegneri, avvocati, esperti di compliance e specialisti in etica.

L'AI Act segna un punto di svolta nell'evoluzione della regolamentazione tecnologica, non solo in Europa ma a livello globale. Le imprese devono affrontare questa sfida con una mentalità proattiva, considerando la compliance non solo come un obbligo legale ma anche come un'opportunità di crescita e innovazione responsabile. Seguendo le linee guida e i principi stabiliti in questo documento, le organizzazioni possono navigare con successo in questo nuovo panorama regolatorio, sfruttando il potenziale dell'IA in modo sicuro, equo e conforme alla legge.

Nelle prossime sezioni della guida, esploreremo in dettaglio ogni aspetto della compliance all'AI Act, fornendo gli strumenti necessari per implementare pratiche solide e mantenere la conformità nel lungo termine.

Considerazioni

Applicazione del Regolamento AI Act a Entità dell'Unione e Sistemi Esclusi

L'AI Act prevede che le istituzioni, gli organi e gli organismi dell'Unione europea, quando agiscono in qualità di fornitori o utilizzatori ("deployer") di un sistema di intelligenza artificiale (IA), debbano conformarsi al regolamento. Questo passaggio sottolinea la necessità di un quadro normativo armonizzato che regoli l'uso dell'IA anche all'interno delle strutture comunitarie. L'obiettivo è evitare discrepanze nella conformità, promuovendo standard comuni per l'uso dell'IA a livello istituzionale.

Sistemi Esclusi dall'Ambito di Applicazione

Uno dei principali punti che il regolamento affronta è la definizione dei casi in cui i sistemi di IA non rientrano nella sua applicazione. In particolare, i sistemi sviluppati o utilizzati per scopi militari, di difesa o di sicurezza nazionale sono esclusi. Questa esclusione è fondata sull'articolo 4, paragrafo 2, del Trattato sull'Unione Europea (TUE), che stabilisce che la sicurezza nazionale rimane di competenza esclusiva degli Stati membri. Le specificità della politica di difesa dell'Unione e le dinamiche geopolitiche richiedono che tali sistemi siano disciplinati dal diritto internazionale pubblico e da normative specifiche per l'uso letale della forza e altre applicazioni militari.

In questo senso, la regolamentazione dei sistemi IA nel contesto militare non rientra nell'AI Act, bensì in ambiti giuridici e normativi che meglio rispondono alle esigenze operative e di sicurezza di tali applicazioni.

Uso Ibrido di Sistemi IA: Applicazione Civile e Militare

Se un sistema IA sviluppato per scopi militari, di difesa o di sicurezza nazionale viene utilizzato temporaneamente o permanentemente per altri scopi, come quelli civili o umanitari, esso rientrerebbe nell'ambito di applicazione dell'AI Act. Questo principio guida le organizzazioni che si trovano ad operare in entrambi gli ambiti, imponendo l'obbligo di garantire la conformità ai requisiti del regolamento per le attività non legate alla sicurezza o alla difesa.

Per esempio, un sistema IA progettato per scopi militari, ma successivamente impiegato per attività di contrasto o in operazioni di sicurezza pubblica, deve rispettare le normative del regolamento. Tuttavia, l'uso di tali sistemi per scopi esclusivamente militari rimane escluso dalla regolamentazione, permettendo agli Stati membri di mantenere flessibilità operativa in queste aree strategiche.

Implicazioni per la Ricerca e Sviluppo (R&S)

Il regolamento tiene conto anche delle attività di ricerca e sviluppo. I sistemi IA sviluppati esclusivamente a scopo di ricerca e sviluppo scientifico sono esclusi dal campo di applicazione dell'AI Act, per garantire che l'innovazione e il progresso tecnico non siano ostacolati da eccessive regolamentazioni. Tuttavia, una volta che questi sistemi vengono immessi sul mercato o messi in servizio, devono rispettare il regolamento.

Ciò riflette un equilibrio tra la promozione dell'innovazione e la necessità di garantire che i sistemi di IA utilizzati a livello commerciale o operativo rispettino gli standard di sicurezza, trasparenza e affidabilità stabiliti dall'AI Act. Anche i test e le sperimentazioni svolti in condizioni reali, noti come spazi di sperimentazione normativa, sono soggetti a questo quadro giuridico, assicurando che non vi siano lacune normative durante la transizione dal prototipo al prodotto finale.

Un Approccio Basato sul Rischio

Il cuore del regolamento AI Act risiede nell'approccio basato sul rischio, che adatta le regole vincolanti in base all'intensità e alla portata dei rischi generati dai diversi sistemi IA. Questa struttura mira a distinguere i sistemi in base alla loro pericolosità potenziale, vietando le pratiche più rischiose e stabilendo requisiti di conformità più severi per i sistemi considerati ad alto rischio.

In questo contesto, le regole sono progettate in modo proporzionato: sistemi IA ad alto rischio, come quelli utilizzati in settori critici come la salute, la sicurezza pubblica o la giustizia, sono soggetti a requisiti più rigorosi rispetto a sistemi IA a basso rischio. Questo garantisce che l'uso dell'IA venga regolamentato in modo da minimizzare i rischi per la società, senza bloccare l'innovazione tecnologica in aree meno critiche.

Il quadro normativo definisce quattro livelli di rischio per i sistemi di intelligenza artificiale, rappresentati come una piramide che illustra i diversi livelli di gravità:

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

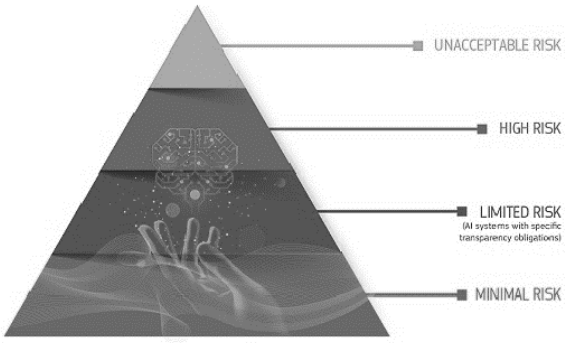


Figura 1: AI Act, *https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-*

Tutti i sistemi di IA che rappresentano una minaccia chiara per la sicurezza, i mezzi di sussistenza e i diritti delle persone sono vietati. Tra questi, si includono pratiche come il punteggio sociale dei cittadini da parte dei governi e giocattoli dotati di assistenza vocale che incoraggiano comportamenti pericolosi.

Rischio elevato

I sistemi di IA considerati ad alto rischio includono tecnologie IA impiegate in diversi settori critici che possono avere un impatto significativo sui diritti fondamentali e sulla sicurezza dei cittadini. Alcuni esempi includono:

- Infrastrutture critiche (ad esempio, i trasporti) che possono mettere a rischio la vita e la salute delle persone.
- Istruzione o formazione professionale, in cui l'IA può influire sull'accesso all'istruzione o determinare il corso professionale di una persona (ad esempio, il punteggio degli esami).
- Componenti di sicurezza dei prodotti, come l'uso dell'IA nella chirurgia assistita da robot.

- Gestione del personale e accesso al lavoro autonomo, come i software di selezione dei CV utilizzati nei processi di reclutamento.
- Servizi essenziali privati e pubblici, come il punteggio di credito che potrebbe negare ai cittadini l'opportunità di ottenere un prestito.
- Forze dell'ordine, dove l'IA può interferire con i diritti fondamentali (ad esempio, valutare l'affidabilità delle prove).
- Gestione della migrazione, asilo e controllo delle frontiere, come l'esame automatizzato delle domande di visto.
- Amministrazione della giustizia e processi democratici, come l'uso di soluzioni IA per la ricerca di sentenze giudiziarie.

I sistemi IA ad alto rischio sono soggetti a obblighi rigorosi prima di essere immessi sul mercato, che includono:

- Valutazioni e sistemi di mitigazione del rischio adeguati.
- Dati di alta qualità per alimentare il sistema, al fine di minimizzare i rischi e gli esiti discriminatori.
- Tracciamento delle attività per garantire la tracciabilità dei risultati.
- Documentazione dettagliata che fornisca tutte le informazioni necessarie sul sistema e sul suo scopo, affinché le autorità possano valutarne la conformità.
- Informazioni chiare e adeguate fornite agli utilizzatori ("deployer").
- Misure di supervisione umana appropriate per ridurre al minimo il rischio.
- Elevati standard di robustezza, sicurezza e precisione.

Identificazione biometrica remota e rischio elevato

Tutti i sistemi di identificazione biometrica remota sono considerati ad alto rischio e soggetti a requisiti stringenti. L'uso di sistemi di identificazione biometrica remota in spazi accessibili al pubblico per scopi di forze dell'ordine è, in linea di principio, proibito.

Sono previste eccezioni rigorosamente definite, come la ricerca di un bambino scomparso, la prevenzione di una minaccia terroristica specifica e imminente, o la localizzazione e identificazione di un autore o sospetto di un reato grave. L'uso di questi sistemi deve essere autorizzato da un organo giudiziario o altro ente indipendente e limitato nel tempo, nella portata geografica e nei database esaminati.

Rischio limitato

I sistemi IA con rischio limitato sono associati alla mancanza di trasparenza nell'uso dell'IA. L'AI Act introduce specifici obblighi di trasparenza per garantire che le persone siano informate quando necessario, favorendo la fiducia nell'IA. Ad esempio: Quando si utilizza un chatbot, le persone devono essere consapevoli che stanno interagendo con una macchina, permettendo loro di decidere se continuare l'interazione o meno.

I fornitori devono garantire che i contenuti generati dall'IA siano identificabili.

I testi generati dall'IA pubblicati con l'intento di informare il pubblico su questioni di interesse pubblico devono essere etichettati come contenuti artificialmente generati. Questo obbligo si applica anche a contenuti audio e video, come i deepfake.

Rischio minimo o nullo

Il regolamento consente il libero utilizzo di sistemi IA a rischio minimo, che comprendono applicazioni come videogiochi con IA integrata o filtri antispam. La maggior parte dei sistemi IA attualmente utilizzati nell'UE rientra in questa categoria.

Come funziona nella “pratica” per i fornitori di sistemi IA ad alto rischio?

Il processo di conformità per i fornitori di sistemi IA ad alto rischio segue un percorso chiaro, che comprende i seguenti passaggi:

- Dichiarazione di conformità: Il fornitore deve dimostrare che il sistema IA soddisfa tutti i requisiti del regolamento.
- Monitoraggio post-mercato: Una volta che il sistema è sul mercato, le autorità competenti effettuano la sorveglianza del mercato, mentre gli utilizzatori garantiscono la supervisione umana e il monitoraggio continuo.
- Segnalazione degli incidenti: I fornitori e gli utilizzatori devono segnalare eventuali incidenti gravi e malfunzionamenti del sistema.

Questo processo garantisce che i sistemi IA ad alto rischio siano costantemente monitorati e adeguatamente gestiti, al fine di ridurre al minimo i rischi per gli utenti e la società.

Commento sulle considerazioni dell’ AI Act

Nel percorso di stesura di questa guida, si è tenuto conto delle principali disposizioni e obblighi contenuti nell'AI Act per supportare il lettore nella comprensione pratica del regolamento e nella sua corretta applicazione. Tuttavia, ritengo che le considerazioni presenti nelle pagine da 1 a 44 del documento ufficiale dell'AI Act, sebbene utili per fornire un'infarinatura generale sulle tematiche normative, non siano essenziali per fini pratici, come eseguire una “compliance” diretta al decreto.

Difatti, queste pagine trattano elementi introduttivi e contestuali, che, pur offrendo una panoramica utile del quadro normativo e delle basi etiche, non forniscono contributi immediatamente operativi per chi cerca di comprendere come applicare il regolamento nella pratica. Per coloro che desiderano esplorare tali aspetti più nel dettaglio, al fine di ampliare le proprie conoscenze generali sulle considerazioni giuridiche e filosofiche che stanno alla base dell'AI Act, suggerisco di consultare il documento ufficiale, disponibile sul sito dell'Unione Europea.

Disposizioni Generali dell'AI Act: Scopo e Obiettivi

L'Articolo 1 del Regolamento AI Act definisce chiaramente lo scopo di questa normativa, ponendo le basi per un quadro giuridico che mira a migliorare il funzionamento del mercato interno dell'Unione Europea, attraverso la promozione di un'intelligenza artificiale (IA) che sia antropocentrica e affidabile. Questo concetto si riferisce a un'IA sviluppata per servire e tutelare l'essere umano, assicurando che la tecnologia rimanga al servizio della dignità e dei diritti fondamentali delle persone.

Uno degli obiettivi centrali del regolamento è garantire un elevato livello di protezione della salute, della sicurezza e dei diritti fondamentali, tra cui la democrazia, lo Stato di diritto e la protezione dell'ambiente, prevenendo gli effetti nocivi che l'IA potrebbe causare. A fianco di queste protezioni, l'AI Act promuove l'innovazione tecnologica, cercando di bilanciare la necessità di regolamentare l'IA con il sostegno alla crescita, soprattutto per le PMI e le start-up.

Il presente regolamento stabilisce, inoltre, una serie di disposizioni specifiche, tra cui:

- Regole armonizzate per l'immissione sul mercato, la messa in servizio e l'uso dei sistemi di IA all'interno dell'Unione Europea.
- Divieti per pratiche di IA ritenute inaccettabili e pericolose.
- Requisiti specifici per i sistemi di IA ad alto rischio, imponendo obblighi precisi agli operatori di tali sistemi per garantire conformità e sicurezza.
- Regole di trasparenza, obbligando determinate categorie di sistemi IA a garantire la tracciabilità e la spiegabilità delle loro operazioni.
- Normative sui modelli di IA ad uso generale, per regolamentare la loro immissione sul mercato.
- Misure per la vigilanza del mercato e per il monitoraggio continuo dell'uso e dell'impatto dei sistemi di IA.

Queste disposizioni forniscono un quadro normativo completo, in grado di proteggere i cittadini e al tempo stesso promuovere l'adozione di un'IA innovativa e responsabile, garantendo una supervisione efficace e incentivando la crescita dell'ecosistema IA europeo.

Ambito di Applicazione del Regolamento AI Act

Il Regolamento AI Act si applica a una vasta gamma di soggetti coinvolti nello sviluppo, nella distribuzione e nell'uso dei sistemi di intelligenza artificiale nell'Unione Europea. In particolare, si rivolge a:

- Fornitori che immettono sul mercato o mettono in servizio sistemi di IA, inclusi quelli non situati nell'Unione ma che forniscono prodotti utilizzati nel suo territorio.
- Deployer (utilizzatori) di sistemi di IA stabiliti o situati nell'Unione.
- Fornitori e deployer con sede in paesi terzi, se l'output dei loro sistemi è utilizzato nell'Unione.
- Importatori e distributori di sistemi di IA.
- Fabbricanti di prodotti che includono sistemi di IA nei loro articoli e li immettono sul mercato con il loro marchio.
- Rappresentanti autorizzati di fornitori non stabiliti nell'Unione.
- Persone interessate che si trovano nell'Unione.

Esclusioni dal Regolamento

Il regolamento non si applica a:

- Sistemi di IA utilizzati esclusivamente per scopi militari, di difesa o di sicurezza nazionale, indipendentemente dalla tipologia di entità che li gestisce.
- Sistemi di IA non immessi sul mercato o non messi in servizio nell'Unione, ma utilizzati per scopi militari o di sicurezza nazionale.
- Autorità pubbliche di paesi terzi o organizzazioni internazionali che usano sistemi di IA nel contesto di cooperazioni con l'Unione o Stati membri, a patto che garantiscano una protezione adeguata dei diritti fondamentali.
- Attività di ricerca e sviluppo che non implicano l'immissione sul mercato o la messa in servizio dei sistemi IA.
- Sistemi di IA open source e licenze libere, salvo quando immessi sul mercato come sistemi ad alto rischio.

Interazione con Altre Normative

Il regolamento tiene conto di altre normative UE, come il GDPR e la direttiva sulla protezione dei consumatori, lasciando impregiudicate le relative

disposizioni. In più, consente agli Stati membri di introdurre norme più favorevoli per la protezione dei diritti dei lavoratori in relazione all'uso dell'IA.

In sintesi, l'AI Act copre un'ampia gamma di operatori nel mercato IA, con precise esclusioni per settori e situazioni particolari, assicurando un quadro armonizzato per la sicurezza e la protezione dei diritti fondamentali nell'Unione Europea.

Definizioni e terminologia

Prima di addentrarci nella guida passo-passo sugli articoli dell'AI Act che influenzano in modo sostanziale la conformità dei software, è fondamentale acquisire una chiara comprensione delle definizioni chiave fornite nell'Articolo 3. Queste definizioni costituiscono la base concettuale del regolamento e sono indispensabili per interpretare correttamente i termini tecnici e applicare con precisione le norme stabilite.

1) «sistema di IA»: 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;

2) «rischio»: la combinazione della probabilità del verificarsi di un danno e la gravità del danno stesso;

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

4) «deployer»: una persona fisica o giuridica, un’autorità pubblica, un’agenzia o un altro organismo che utilizza un sistema di IA sotto la propria autorità, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale;

5) «rappresentante autorizzato»: una persona fisica o giuridica ubicata o stabilita nell'Unione che ha ricevuto e accettato un mandato scritto da un fornitore di un sistema di IA o di un modello di IA per finalità generali al fine, rispettivamente, di adempiere ed eseguire per suo conto gli obblighi e le procedure stabiliti dal presente regolamento;

6) «importatore»: una persona fisica o giuridica ubicata o stabilita nell'Unione che immette sul mercato un sistema di IA recante il nome o il marchio di una persona fisica o giuridica stabilita in un paese terzo;

7) «distributore»: una persona fisica o giuridica nella catena di approvvigionamento, diversa dal fornitore o dall'importatore, che mette a disposizione un sistema di IA sul mercato dell'Unione;

8) «operatore»: un fornitore, un fabbricante del prodotto, un deployer, un rappresentante autorizzato, un importatore o un distributore;

9) «immissione sul mercato»: la prima messa a disposizione di un sistema di IA o di un modello di IA per finalità generali sul mercato dell'Unione;

10) «messa a disposizione sul mercato»: la fornitura di un sistema di IA o di un modello di IA per finalità generali per la distribuzione o l'uso sul mercato dell'Unione nel corso di un'attività commerciale, a titolo oneroso o gratuito;

11) «messa in servizio»: la fornitura di un sistema di IA direttamente al deployer per il primo uso o per uso proprio nell'Unione per la finalità prevista;

12) «finalità prevista»: l'uso di un sistema di IA previsto dal fornitore, compresi il contesto e le condizioni d'uso specifici, come dettagliati nelle informazioni comunicate dal fornitore nelle istruzioni per l'uso, nel materiale promozionale o di vendita e nelle dichiarazioni, nonché nella documentazione tecnica;

13) «uso improprio ragionevolmente prevedibile»: l'uso di un sistema di IA in un modo non conforme alla sua finalità prevista, ma che può derivare da un comportamento umano o da un'interazione con altri sistemi, ivi compresi altri sistemi di IA, ragionevolmente prevedibile;

14) «componente di sicurezza»: un componente di un prodotto o di un sistema di IA che svolge una funzione di sicurezza per tale prodotto o sistema di IA o il cui guasto o malfunzionamento mette in pericolo la salute e la sicurezza di persone o beni;

15) «istruzioni per l'uso»: le informazioni comunicate dal fornitore per informare il deployer in particolare della finalità prevista e dell'uso corretto di un sistema di IA;

16) «richiamo di un sistema di IA»: qualsiasi misura volta a ottenere la restituzione al fornitore, la messa fuori servizio o la disabilitazione dell'uso di un sistema di IA messo a disposizione dei deployer;

17) «ritiro di un sistema di IA»: qualsiasi misura volta a impedire che un sistema di IA nella catena di approvvigionamento sia messo a disposizione sul mercato;

18) «prestazioni di un sistema di IA»: la capacità di un sistema di IA di conseguire la finalità prevista;

19) «autorità di notifica»: 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;

20) «valutazione della conformità»: la procedura atta a dimostrare se i requisiti di cui al capo III, sezione 2, relativi a un sistema di IA ad alto rischio sono stati soddisfatti;

21) «organismo di valutazione della conformità»: un organismo che svolge per conto di terzi attività di valutazione della conformità, incluse prove, certificazioni e ispezioni;

22) «organismo notificato»: un organismo di valutazione della conformità notificato in conformità del presente regolamento e di altre pertinenti normative di armonizzazione dell'Unione;

23) «modifica sostanziale»: una modifica di un sistema di IA a seguito della sua immissione sul mercato o messa in servizio che non è prevista o programmata nella valutazione iniziale della conformità effettuata dal fornitore e che ha l'effetto di incidere sulla conformità del sistema di IA ai requisiti di cui al capo III, sezione 2, o comporta una modifica della finalità prevista per la quale il sistema di IA è stato valutato;

24) «marcatura CE»: una marcatura mediante la quale un fornitore indica che un sistema di IA è conforme ai requisiti stabiliti al capo III, sezione 2, e in altre normative di armonizzazione dell'Unione applicabili e che ne prevedono l'apposizione;

25) «sistema di monitoraggio successivo all'immissione sul mercato»: tutte le attività svolte dai fornitori di sistemi di IA al fine di raccogliere e analizzare l'esperienza maturata tramite l'uso dei sistemi di IA che immettono sul mercato o che mettono in servizio, al fine di individuare eventuali necessità di immediate azioni correttive o preventive;

26) «autorità di vigilanza del mercato»: l'autorità nazionale che svolge le attività e adotta le misure a norma del regolamento (UE) 2019/1020;

27) «norma armonizzata»: la norma armonizzata di cui all'articolo 2, punto 1), lettera c), del regolamento (UE) n, 1025/2012;

28) «specifiche comuni»: un insieme di specifiche tecniche quali definite all'articolo 2, punto 4), del regolamento (UE) n, 1025/2012, che forniscono i mezzi per soddisfare determinati requisiti stabiliti a norma del presente regolamento;

29) «dati di addestramento»: i dati utilizzati per addestrare un sistema di IA adattandone i parametri che può apprendere;

30) «dati di convalida»: i dati utilizzati per fornire una valutazione del sistema di IA addestrato e per metterne a punto, tra l'altro, i parametri che non può apprendere e il processo di apprendimento, al fine tra l'altro di evitare lo scarso (under fitting) o l'eccessivo (over fitting) adattamento ai dati di addestramento;

31) «set di dati di convalida»: un set di dati distinto o costituito da una partizione fissa o variabile del set di dati di addestramento;

32) «dati di prova»: i dati utilizzati per fornire una valutazione indipendente del sistema di IA al fine di confermarne le prestazioni attese prima della sua immissione sul mercato o messa in servizio;

33) «dati di input»: i dati forniti a un sistema di IA o direttamente acquisiti dallo stesso, in base ai quali il sistema produce un output;

34) «dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, quali le immagini facciali o i dati dattiloscopici;

35) «identificazione biometrica»: il riconoscimento automatizzato delle caratteristiche umane fisiche, fisiologiche, comportamentali o psicologiche allo scopo di determinare l'identità di una persona fisica confrontando i suoi dati biometrici con quelli di individui memorizzati in una banca dati;

36) «verifica biometrica»: la verifica automatizzata e uno a uno, inclusa l'autenticazione, dell'identità di persone fisiche mediante il confronto dei loro dati biometrici con i dati biometrici forniti in precedenza;

37) «categorie particolari di dati personali»: le categorie di dati personali di cui all'articolo 9, paragrafo 1, del regolamento (UE) 2016/679, all'articolo 10 della direttiva (UE) 2016/680 e all'articolo 10, paragrafo 1, del regolamento (UE) 2018/1725;

38) «dati operativi sensibili»: dati operativi relativi ad attività di prevenzione, accertamento, indagine o perseguimento di reati, la cui divulgazione potrebbe compromettere l'integrità dei procedimenti penali;

39) «sistema di riconoscimento delle emozioni»: un sistema di IA finalizzato all'identificazione o all'inferenza di emozioni o intenzioni di persone fisiche sulla base dei loro dati biometrici;

40) «sistema di categorizzazione biometrica»: un sistema di IA che utilizza i dati biometrici di persone fisiche al fine di assegnarle a categorie specifiche, a meno che non sia accessorio a un altro servizio commerciale e strettamente necessario per ragioni tecniche oggettive;

41) «sistema di identificazione biometrica remota»: un sistema di IA finalizzato all'identificazione di persone fisiche, senza il loro coinvolgimento attivo, tipicamente a distanza mediante il confronto dei dati biometrici di una persona con i dati biometrici contenuti in una banca dati di riferimento;

42) «sistema di identificazione biometrica remota in tempo reale»: un sistema di identificazione biometrica remota in cui il rilevamento dei dati biometrici, il confronto e l'identificazione avvengono senza ritardi significativi, il quale comprende non solo le identificazioni istantanee, ma anche quelle che avvengono con brevi ritardi limitati al fine di evitare l'elusione;

43) «sistema di identificazione biometrica remota a posteriori»: un sistema di identificazione biometrica remota diverso da un sistema di identificazione biometrica remota «in tempo reale»;

44) «spazio accessibile al pubblico»: qualsiasi luogo fisico di proprietà pubblica o privata accessibile a un numero indeterminato di persone fisiche, indipendentemente dal fatto che possano applicarsi determinate condizioni di accesso e indipendentemente dalle potenziali restrizioni di capacità;

45) «autorità di contrasto»: a) qualsiasi autorità pubblica competente in materia di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro le minacce alla sicurezza pubblica e la prevenzione delle stesse; oppure

b) qualsiasi altro organismo o entità incaricati dal diritto dello Stato membro di esercitare l'autorità pubblica e i poteri pubblici a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro le minacce alla sicurezza pubblica e la prevenzione delle stesse;

46) «attività di contrasto»: le attività svolte dalle autorità di contrasto o per loro conto a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro le minacce alla sicurezza pubblica e la prevenzione delle stesse;

47) «ufficio per l'IA»: la funzione della Commissione volta a contribuire all'attuazione, al monitoraggio e alla supervisione dei sistemi di IA e dei modelli di IA per finalità generali, e della governance dell'IA prevista dalla decisione della Commissione del 24 gennaio 2024. I riferimenti all'ufficio per l'IA contenuti nel presente regolamento si intendono fatti alla Commissione;

48) «autorità nazionale competente»: un'autorità di notifica o un'autorità di vigilanza del mercato; per quanto riguarda i sistemi di IA messi in servizio o utilizzati da istituzioni, organi e organismi dell'Unione, i riferimenti alle autorità nazionali competenti o alle autorità di vigilanza del mercato contenuti nel presente regolamento si intendono fatti al Garante europeo della protezione dei dati;

49) «incidente grave»: un incidente o malfunzionamento di un sistema di IA che, direttamente o indirettamente, causa una delle conseguenze seguenti:

a) il decesso di una persona o gravi danni alla salute di una persona;

b) una perturbazione grave e irreversibile della gestione o del funzionamento delle infrastrutture critiche;

c) la violazione degli obblighi a norma del diritto dell'Unione intesi a proteggere i diritti fondamentali;

d) gravi danni alle cose o all'ambiente;

50) «dati personali»: i dati personali quali definiti all'articolo 4, punto 1), del regolamento (UE) 2016/679;

51) «dati non personali»: dati diversi dai dati personali di cui all'articolo 4, punto 1), del regolamento (UE) 2016/679;

52) «profilazione»: la profilazione quale definita all'articolo 4, punto 4), del regolamento (UE) 2016/679;

53) «piano di prova in condizioni reali»: un documento che descrive gli obiettivi, la metodologia, l'ambito geografico, della popolazione e temporale, il monitoraggio, l'organizzazione e lo svolgimento della prova in condizioni reali;

54) «piano dello spazio di sperimentazione»: un documento concordato tra il fornitore partecipante e l'autorità competente in cui sono descritti gli obiettivi, le condizioni, il calendario, la metodologia e i requisiti relativamente alle attività svolte all'interno dello spazio di sperimentazione;

55) «spazio di sperimentazione normativa per l'IA»: un quadro controllato istituito da un'autorità competente che offre ai fornitori o potenziali fornitori di sistemi di IA la possibilità di sviluppare, addestrare, convalidare e provare, se del caso in condizioni reali, un sistema di IA innovativo, conformemente a un piano dello spazio di sperimentazione per un periodo di tempo limitato sotto supervisione regolamentare;

56) «alfabetizzazione in materia di IA»: le competenze, le conoscenze e la comprensione che consentono ai fornitori, ai deployer e alle persone interessate, tenendo conto dei loro rispettivi diritti e obblighi nel contesto del presente regolamento, di procedere a una diffusione informata dei sistemi di IA, nonché di acquisire consapevolezza in merito alle opportunità e ai rischi dell'IA e ai possibili danni che essa può causare;

57) «prova in condizioni reali»: la prova temporanea di un sistema di IA per la sua finalità prevista in condizioni reali al di fuori di un laboratorio o di un ambiente altrimenti simulato al fine di raccogliere dati affidabili e solidi e di valutare e verificare la conformità del sistema di IA ai requisiti del presente regolamento e che non è considerata immissione sul mercato o messa in servizio del sistema di IA ai sensi del presente regolamento, purché siano soddisfatte tutte le condizioni di cui all'articolo 57 o 60;

58) «soggetto»: ai fini della prova in condizioni reali, una persona fisica che partecipa a prove in condizioni reali;

59) «consenso informato»: l'espressione libera, specifica, inequivocabile e volontaria di un soggetto della propria disponibilità a partecipare a una determinata prova in condizioni reali, dopo essere stato informato di tutti gli aspetti della prova rilevanti per la sua decisione di partecipare;

60) «deep fake»: un'immagine o un contenuto audio o video generato o manipolato dall'IA che assomiglia a persone, oggetti, luoghi, entità o eventi esistenti e che apparirebbe falsamente autentico o veritiero a una persona;

61) «infrazione diffusa»: qualsiasi azione od omissione contraria al diritto dell'Unione che tutela gli interessi delle persone:

a) che abbia arrecato o possa arrecare un danno agli interessi collettivi di persone che risiedono in almeno due Stati membri diversi dallo Stato membro in cui:

i) ha avuto origine o si è verificato l'azione o l'omissione in questione;

ii) è ubicato o stabilito il fornitore interessato o, se del caso, il suo rappresentante autorizzato; oppure

iii) è stabilito il deployer, quando la violazione è commessa dal deployer;

b) che abbia arrecato, arrechi o possa arrecare un danno agli interessi collettivi di persone e che presenti caratteristiche comuni, compresa la stessa pratica illecita e lo stesso interesse leso e che si verifichi simultaneamente, commessa dal medesimo operatore, in almeno tre Stati membri;

62) «infrastruttura critica»: infrastruttura critica quale definita all'articolo 2, punto 4), della direttiva (UE) 2022/2557;

63) «modello di IA per finalità generali»: un modello di IA, anche laddove tale modello di IA sia addestrato con grandi quantità di dati utilizzando l'auto supervisione su larga scala, che sia caratterizzato una generalità significativa e sia in grado di svolgere con competenza un'ampia gamma di compiti distinti, indipendentemente dalle modalità con cui il modello è immesso sul mercato, e che può essere integrato in una varietà di sistemi o applicazioni a valle, ad eccezione dei modelli di IA utilizzati per attività di ricerca, sviluppo o prototipazione prima di essere immessi sul mercato;

64) «capacità di impatto elevato»: capacità che corrispondono o superano le capacità registrate nei modelli di IA per finalità generali più avanzati;

65) «rischio sistemico»: un rischio specifico per le capacità di impatto elevato dei modelli di IA per finalità generali, avente un impatto significativo sul mercato dell'Unione a causa della sua portata o di effetti negativi effettivi o ragionevolmente prevedibili sulla salute pubblica, la sicurezza, i diritti

fondamentali o la società nel suo complesso, che può propagarsi su larga scala lungo l'intera catena del valore;

66) «sistema di IA per finalità generali»: un sistema di IA basato su un modello di IA per finalità generali e che ha la capacità di perseguire varie finalità, sia per uso diretto che per integrazione in altri sistemi di IA;

67) «operazione in virgola mobile»: qualsiasi operazione o assegnazione matematica che comporta numeri in virgola mobile, un sottoinsieme dei numeri reali generalmente rappresentati sui computer mediante un numero intero con precisione fissa avente come fattore di scala un esponente intero di una base fissa;

68) «fornitore a valle»: un fornitore di un sistema di IA, compreso un sistema di IA per finalità generali, che integra un modello di IA, indipendentemente dal fatto che il modello di IA sia fornito dallo stesso e integrato verticalmente o fornito da un'altra entità sulla base di relazioni contrattuali.

Le definizioni fornite dall'Articolo 3 dell'AI Act costituiscono la base terminologica per l'intero regolamento. Comprendere chiaramente queste definizioni è essenziale per garantire la conformità ai requisiti imposti dalla normativa. Nel proseguo della guida, ci concentreremo sugli articoli che hanno un impatto diretto e materiale sulla compliance, aiutando fornitori, deployer e altre entità a navigare le complesse disposizioni del regolamento.

Guida per la Conformità ai Requisiti Normativi in Materia di IA

Questa guida è stata concepita per aiutare le organizzazioni a garantire la conformità alle normative in materia di intelligenza artificiale (IA). Ogni articolo di legge viene analizzato ed esaminato sotto forma di domande, che permettono di valutare facilmente se l'organizzazione sta rispettando i requisiti imposti. Queste domande non costituiscono un semplice questionario, ma rappresentano un metodo pratico per affrontare ciascun articolo, individuando eventuali lacune e aree di miglioramento.

In aggiunta, è stata effettuata una classificazione delle domande per facilitare la comprensione del loro livello di rilevanza:

- **Critiche:** Domande che devono essere soddisfatte per garantire la conformità e/o che sono di significativa rilevanza. Una risposta negativa a queste domande significa non conformità.
- **Importanti**: Domande che, sebbene non critiche, sono molto rilevanti. Una risposta negativa richiede attenzione e azioni correttive, ma non determina immediatamente la non conformità.
- **Consigliate:** Domande che rappresentano buone pratiche. Una risposta negativa indica un'area di miglioramento, ma non compromette la conformità complessiva.

Inoltre, va considerato che:

- Le risposte negative da parte dei lettori di questa guida a domande critiche identificano una non conformità che deve essere immediatamente risolta per evitare rischi legali e operativi.
- Le risposte negative da parte dei lettori a domande importanti indicano una necessità di miglioramento, ma non implicano una violazione immediata.

Ho personalmente individuato che i seguenti articoli presentano un impatto materiale significativo e richiedono particolare attenzione: **4, 5, 6, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 42, 43, 47, 48, 49, 50, 51, 52, 53, 54, 55.** Gli articoli mancanti non sono stati esclusi per errore, ma perché non ritenuti impattanti sulla conformità di un software al decreto. Essi trattano principalmente tematiche relative agli Stati o a direttive che coinvolgono la Commissione e gli enti incaricati della messa in pratica dell'AI Act, e non influenzano direttamente le responsabilità di chi sviluppa o implementa sistemi di IA a livello aziendale.

Alfabetizzazione in materia di IA - Comprendere e Applicare l'Articolo 4

Questo articolo si concentra sull'assicurare che tutto il personale coinvolto nell'uso, distribuzione o funzionamento dei sistemi di IA riceva la formazione tecnica necessaria. L'obiettivo principale è garantire che chiunque gestisca i sistemi di IA abbia un livello di comprensione sufficiente, sia in termini di conoscenze personali che nel contesto specifico in cui questi sistemi vengono utilizzati.

# Articolo	Domanda	Livello di criticità	Richieste legislatore
4	Il personale coinvolto nell'uso dei sistemi di IA ha ricevuto una formazione tecnica adeguata?	Critico	*Articolo 4* *Alfabetizzazione in materia di IA I fornitori e i deployer dei sistemi di IA adottano misure per garantire nella misura del possibile un livello sufficiente di alfabetizzazione in materia di IA del loro personale nonché di qualsiasi altra persona che si occupa del funzionamento e dell'utilizzo dei sistemi di IA per loro conto, prendendo in considerazione le loro conoscenze tecniche, la loro esperienza, istruzione e formazione, nonché il contesto in cui i sistemi di IA devono essere utilizzati, e tenendo conto delle persone o dei gruppi di persone su cui i sistemi di IA devono essere utilizzati*
4	Sono disponibili e implementati programmi di formazione continua in materia di IA per il personale?	Critico	
4	È stato valutato il background educativo e l'esperienza del personale nell'ambito dell'IA?	Importante	
4	Esistono programmi specifici di alfabetizzazione in materia di IA per tutti i soggetti coinvolti?	Importante	
4	È stata effettuata una valutazione del contesto specifico in cui verranno utilizzati i sistemi di IA?	Consigliato	
4	Esiste una documentazione aggiornata che attesta i livelli di alfabetizzazione del personale in materia di IA?	Consigliato	

Pratiche di IA vietate - Comprendere e Applicare l'Articolo 5

Questo capitolo si concentra sulle pratiche relative all'uso dell'intelligenza artificiale che sono esplicitamente vietate dalle normative. L'IA, se non utilizzata correttamente, può violare i diritti fondamentali delle persone e causare gravi ripercussioni. Pertanto, è cruciale che le organizzazioni evitino queste pratiche proibite, per proteggere i diritti umani e rispettare le leggi in materia di intelligenza artificiale.

# Articolo	Domanda	Livello di criticità	Richieste legislatore
5	Il sistema di IA utilizza tecniche subliminali che agiscono senza che una persona ne sia consapevole?	Critico	*Sono vietati sistemi di IA che utilizzano tecniche subliminali o tecniche volutamente manipolative o ingannevoli con lo scopo di distorcere il comportamento delle persone, influenzando le loro decisioni in un modo che potrebbe causare danni significativi.* *(Par. 1(a) Art. 5)*
5	Il vostro sistema di IA sfrutta vulnerabilità come l'età, la disabilità o la condizione sociale delle persone per influenzare il loro comportamento?	Critico	*È vietato immettere sul mercato, mettere in servizio o utilizzare sistemi di IA che sfruttano le vulnerabilità di specifici gruppi di persone, come minori o persone con disabilità, per distorcere il loro comportamento in modo tale da poter causare danni significativi.* *(Par. 1(b) Art. 5)*
5	Il vostro sistema di IA assegna un "punteggio sociale" alle persone in base al loro comportamento o alle loro caratteristiche personali?	Critico	*Sono vietati i sistemi di IA che assegnano un punteggio sociale alle persone sulla base del loro comportamento o delle loro caratteristiche personali, risultando in trattamenti discriminatori o svantaggiati in contesti non collegati.* *(Par. 1(c) Art. 5)*
5	Il vostro sistema di IA prevede se una persona potrebbe commettere un reato basandosi solo su dati personali o caratteristiche della personalità?	Critico	*È vietato l'uso di sistemi di IA per prevedere se una persona commetterà un reato basandosi esclusivamente su dati personali o su caratteristiche della personalità, a meno che non sia in supporto a una valutazione umana basata su fatti oggettivi e verificabili.* *(Par. 1(d) Art. 5)*

5	Il vostro sistema di IA raccoglie o utilizza immagini facciali da Internet o telecamere senza una specifica autorizzazione?	Critico	*È vietato immettere sul mercato, mettere in servizio o utilizzare sistemi di IA che creano o ampliano banche dati di riconoscimento facciale tramite il scraping non mirato di immagini facciali da Internet o da filmati di telecamere senza autorizzazione."* *(Par. 1(e) Art. 5)*
5	Il vostro sistema di IA rileva le emozioni delle persone in luoghi di lavoro o scuole senza un motivo medico o di sicurezza? Tranne laddove l'uso del sistema di IA sia destinato a essere messo in funzione o immesso sul mercato per motivi medici o di sicurezza	Critico	*È vietato immettere sul mercato, mettere in servizio o utilizzare sistemi di IA per inferire le emozioni delle persone in contesti come luoghi di lavoro o istituti di istruzione, a meno che non vi siano motivi medici o di sicurezza che giustifichino tale uso. (Par. 1(f) Art. 5)*
5	Il vostro sistema di IA usa dati biometrici per fare deduzioni su razza, opinioni politiche, religione, orientamento sessuale o altre caratteristiche personali (es. appartenenza sindacale, convinzioni religiose o filosofiche, vita sessuale)?	Critico	*È vietato l'uso di sistemi di categorizzazione biometrica che utilizzano dati biometrici per fare deduzioni su razza, opinioni politiche, orientamento sessuale, religione, appartenenza sindacale o altre caratteristiche personali. (Par. 1(g) Art. 5)*
5	Utilizzate sistemi di identificazione biometrica "in tempo reale" in spazi pubblici senza una ragione specifica e autorizzata? Le ragioni specifiche ed autorizzate sono le seguenti: i) la ricerca mirata di specifiche vittime di sottrazione, tratta di esseri umani o sfruttamento sessuale di esseri umani, nonché la ricerca di persone scomparse; ii) la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di una minaccia reale e attuale o reale e prevedibile di un attacco terroristico; iii) la localizzazione o l'identificazione di una persona sospettata di aver commesso un reato, ai fini dello svolgimento di un'indagine penale, o dell'esercizio di un'azione penale	Critico	*L'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi pubblici è vietato a meno che non sia strettamente necessario per obiettivi specifici, come la ricerca di vittime di crimini, la prevenzione di attacchi terroristici o la localizzazione di sospettati. (Par. 1(h) Art. 5)*

	o dell'esecuzione di una sanzione penale per i reati di cui all'allegato II, punibile nello Stato membro interessato con una pena o una misura di sicurezza privativa della libertà della durata massima di almeno quattro anni		
5	Avete ottenuto un'autorizzazione preventiva da un'autorità giudiziaria o amministrativa indipendente per utilizzare sistemi di identificazione biometrica remota "in tempo reale" in spazi pubblici?	Critico	*L'uso di sistemi di identificazione biometrica remota "in tempo reale" richiede un'autorizzazione preventiva da parte di un'autorità giudiziaria o amministrativa indipendente, la cui decisione è vincolante. (Par. 3 Art. 5)*
5	È stata condotta una valutazione dell'impatto sui diritti fondamentali prima di utilizzare sistemi di identificazione biometrica remota "in tempo reale" in spazi pubblici?	Critico	*Prima dell'uso di sistemi di identificazione biometrica remota "in tempo reale", è richiesta una valutazione dell'impatto sui diritti fondamentali, conformemente alle regole nazionali. (Par. 3 Art. 5)*
5	Avete considerato la gravità, la probabilità e l'entità dei danni che potrebbero derivare dall'uso di sistemi di identificazione biometrica in spazi pubblici?	Importante	*Ogni uso di sistemi di identificazione biometrica remota deve considerare la gravità, la probabilità e l'entità dei danni che potrebbero verificarsi in caso di mancato uso del sistema. (Par. 2(a) Art. 5)*

5	In caso di urgenza, avete avviato l'uso del sistema senza autorizzazione e poi richiesto l'autorizzazione entro 24 ore come previsto? Ogniuso di un sistema di identificazione biometrica remota «in tempo reale» in spazi accessibili al pubblico a fini di attività di contrasto è subordinato a un'autorizzazione preventiva rilasciata da un'autorità giudiziaria oda un'autorità amministrativa indipendente, la cui decisione è vincolante, dello Stato membro in cui deve avvenire l'uso, rilasciata su richiesta motivata e in conformità delle regole dettagliate del diritto nazionale di cui al paragrafo 5. Tuttavia, in una situazione di urgenza debitamente giustificata, è possibile iniziare a usare il sistema senza autorizzazione a condizione che tale autorizzazione sia richiesta senza indebito ritardo, al più tardi entro 24 ore. Se tale autorizzazione è respinta, l'uso è interrotto con effetto immediato e tutti i dati nonché i risultati e gli output di tale uso sono immediatamente eliminati e cancellati	Importante	*Questo punto riguarda la gestione di situazioni di urgenza in cui l'uso di sistemi di identificazione biometrica remota "in tempo reale" potrebbe essere necessario senza un'autorizzazione preventiva. La classificazione come "Importante" riflette il fatto che, sebbene sia cruciale seguire le regole (richiedere l'autorizzazione entro 24 ore, interrompere l'uso immediatamente se l'autorizzazione viene negata, e cancellare i dati), la possibilità di avviare l'uso del sistema senza autorizzazione preventiva è contemplata dal regolamento stesso. Quindi, c'è un margine di flessibilità concesso in situazioni specifiche, che riduce leggermente la criticità rispetto ad altri punti dove la conformità è assolutamente necessaria in ogni caso. "In casi di urgenza debitamente giustificati, è possibile avviare l'uso del sistema senza autorizzazione, a condizione che l'autorizzazione venga richiesta entro 24 ore. Se rifiutata, l'uso deve cessare immediatamente e tutti i dati devono essere eliminati." (Par. 3 Art. 5)*
5	Il vostro uso dei sistemi di identificazione biometrica rispetta le limitazioni temporali, geografiche e personali previste dalle leggi nazionali?	Importante	*L'uso di sistemi di identificazione biometrica remota deve rispettare le limitazioni temporali, geografiche e personali stabilite dalle leggi nazionali. (Par. 2(b) Art. 5)*

5	Avete notificato l'uso di sistemi di identificazione biometrica alle autorità di vigilanza e di protezione dei dati come richiesto?	Importante	*La notifica alle autorità di vigilanza e di protezione dei dati è essenziale per garantire la trasparenza e la responsabilità dell'uso dei sistemi di identificazione biometrica. Tuttavia, la mancata notifica non necessariamente implica un uso immediatamente pericoloso o illegale del sistema stesso. Anche se la mancata notifica costituisce una non conformità, essa può essere considerata "Importante" piuttosto che "Critica" perché, teoricamente, il sistema potrebbe essere conforme in tutti gli altri aspetti più rilevanti (come l'ottenimento dell'autorizzazione, l'uso proporzionato, ecc.) ma solo mancare di questo passaggio procedurale. In altre parole, l'omissione della notifica può essere un problema grave, ma non implica automaticamente un danno diretto o un uso illecito di IA come potrebbero fare altre violazioni.*

Regole di classificazione per i sistemi di IA ad alto rischio - Comprendere e Applicare l'Articolo 6

# Articolo	Domanda	Livello di criticità	Richieste legislatore
6	Il vostro sistema di IA è destinato a essere utilizzato come componente di sicurezza di un prodotto, o è esso stesso un prodotto disciplinato dalla normativa di armonizzazione dell'Unione elencata nell'allegato I del regolamento?	Ad alto rischio se soddisfatte entrambe le condizioni	*I sistemi di IA destinati a essere utilizzati come componenti di sicurezza di prodotti disciplinati dalla normativa di armonizzazione dell'Unione elencata nell'Allegato I sono classificati come ad alto rischio. (Par. 1(a) Art. 6)*
6	Il prodotto che contiene il vostro sistema di IA come componente di sicurezza, o il sistema di IA stesso in quanto prodotto, è soggetto a una valutazione di conformità da parte di terzi per l'immissione sul mercato o la messa in servizio ai sensi della normativa di armonizzazione dell'Unione elencata nell'allegato I del regolamento?		*Quando un sistema di IA è utilizzato come componente di sicurezza di prodotti disciplinati dalla normativa di armonizzazione dell'Unione, tale sistema è soggetto a una valutazione di conformità prima dell'immissione sul mercato o della messa in servizio. (Par. 1(a) Art. 6*
6	Il vostro sistema di IA rientra tra quelli elencati nell'allegato III del regolamento, classificati come "ad alto rischio"?	Alto rischio	*I sistemi di IA elencati nell'Allegato III del regolamento, che incidono su diritti e sicurezza fondamentali, sono classificati come ad alto rischio. (Par. 2(a) Art. 6)*

6	Se il sistema di IA rientra nell'Allegato III, verifica se non presenta un rischio significativo di danno per la salute, la sicurezza o i diritti fondamentali delle persone fisiche, né influisce materialmente sul risultato di un processo decisionale: Se "Sì", almeno una delle seguenti condizioni deve essere soddisfatta: a) Il sistema di IA è destinato a eseguire un compito procedurale limitato? Sì / No b) Il sistema di IA è destinato a migliorare il risultato di un'attività umana precedentemente completata? Sì / No c) 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? Sì / No d) Il sistema di IA è destinato a eseguire un compito preparatorio per una valutazione pertinente ai casi d'uso elencati nell'Allegato III? Sì / No Nota: Se una delle condizioni dalla 3a alla 3d è soddisfatta, il sistema può non essere considerato "ad alto rischio". Tuttavia, se la risposta alla prossima domanda è "Sì", il sistema è comunque ad alto rischio.	Alto rischio	*Un sistema di IA elencato nell'Allegato III può essere escluso dalla classificazione di alto rischio se è destinato a svolgere compiti procedurali limitati, migliorare un'attività umana o rilevare deviazioni da schemi decisionali esistenti, senza sostituire la valutazione umana.(Par. 2(b) Art. 6)*
6	Il sistema di IA di cui all'Allegato III effettua profilazione di persone fisiche? Se "Sì", il sistema è sempre considerato "ad alto rischio".	Alto rischio	

6	Se il fornitore ritiene che il sistema di IA di cui all'Allegato III non sia ad alto rischio, ha documentato la valutazione prima che il sistema sia immesso sul mercato o messo in servizio?	Importante	*Un fornitore che ritiene che un sistema di IA di cui all'allegato III non sia ad alto rischio ne documenta la valutazione prima che tale sistema sia immesso sul mercato oppure messo in servizio. Tale fornitore è soggetto all'obbligo di registrazione di cui all'articolo 49, paragrafo 2. Su richiesta delle autorità nazionali competenti, il fornitore mette a disposizione la documentazione relativa alla valutazione (Par. 4 Art. 6)*
6	Se il fornitore ritiene che il sistema di IA di cui all'Allegato III non sia ad alto rischio, ha rispettato l'obbligo di registrazione del sistema di IA ai sensi dell'articolo 49, paragrafo 2?	Importante	*Un fornitore che ritiene che un sistema di IA di cui all'allegato III non sia ad alto rischio ne documenta la valutazione prima che tale sistema sia immesso sul mercato oppure messo in servizio. Tale fornitore è soggetto all'obbligo di registrazione di cui all'articolo 49, paragrafo 2. Su richiesta delle autorità nazionali competenti, il fornitore mette a disposizione la documentazione relativa alla valutazione (Par. 4 Art. 6)*
6	Il fornitore è in grado di mettere a disposizione delle autorità nazionali competenti la documentazione relativa alla valutazione del sistema?	Importante	*Un fornitore che ritiene che un sistema di IA di cui all'allegato III non sia ad alto rischio ne documenta la valutazione prima che tale sistema sia immesso sul mercato oppure messo in servizio. Tale fornitore è soggetto all'obbligo di registrazione di cui all'articolo 49, paragrafo 2. Su richiesta delle autorità nazionali competenti, il fornitore mette a disposizione la documentazione relativa alla valutazione (Par. 4 Art. 6)*

Conformità ai requisiti - Comprendere e Applicare l'Articolo 8

# Articolo	Domanda	Livello di criticità	Richieste legislatore
8	I sistemi di IA ad alto rischio rispettano i requisiti stabiliti, tenendo conto delle loro finalità previste e dello stato dell'arte generalmente riconosciuto in materia di IA e tecnologie correlate?	Importante	*È necessario considerare anche il sistema di gestione dei rischi di cui all'Articolo 9 del regolamento.*
8	Se un prodotto contiene un sistema di IA cui si applicano sia i requisiti del regolamento sull'AI Act sia quelli della normativa di armonizzazione dell'Unione elencata nell'Allegato I, Sezione A, il fornitore garantisce che il prodotto sia conforme a tutti i requisiti applicabili?	Importante	
8	Il fornitore ha integrato i processi di prova e comunicazione necessari, nonché le informazioni e la documentazione fornite relativamente al prodotto, nella documentazione e nelle procedure esistenti richieste dalla normativa di armonizzazione dell'Unione per evitare duplicazioni e ridurre al minimo gli oneri aggiuntivi?	Importante	

Sistema di gestione dei rischi - Comprendere e Applicare l'Articolo 9

# Articolo	Domanda	Livello di criticità	Richieste legislatore
9	È stato istituito, attuato, documentato e mantenuto un sistema di gestione dei rischi per il sistema di IA ad alto rischio?	Importante	
9	Il sistema di gestione dei rischi è un processo iterativo e continuo pianificato ed eseguito per l'intero ciclo di vita del sistema di IA, con riesame e aggiornamento costanti e sistematici?	Importante	
9	Il sistema di gestione dei rischi comprende le seguenti fasi: a) Identificazione e analisi dei rischi noti e ragionevolmente prevedibili che il sistema di IA può porre per la salute, la sicurezza e i diritti fondamentali? Sì / No b) Stima e valutazione dei rischi che possono emergere durante l'uso conforme alla finalità prevista e in condizioni di uso improprio ragionevolmente prevedibile? Sì / No c) Valutazione di altri rischi derivanti dall'analisi dei dati raccolti dal sistema di monitoraggio post-commercializzazione? Sì / No d) Adozione di misure di gestione dei rischi adeguate e mirate per affrontare i rischi identificati? Sì / No	Importante	
9	Le misure di gestione dei rischi considerano l'effetto e l'interazione dei requisiti per minimizzare i rischi in modo efficace e raggiungere un equilibrio adeguato tra le diverse misure di conformità?	Importante	
9	Le misure di gestione dei rischi garantiscono che i rischi residui associati a ciascun pericolo e il rischio complessivo siano considerati accettabili?	Importante	

9	Il fornitore garantisce che: a) I rischi siano eliminati o ridotti per quanto tecnicamente possibile tramite una progettazione adeguata del sistema di IA? Sì / No b) Siano implementate misure di attenuazione e controllo per affrontare i rischi che non possono essere eliminati? Sì / No c) Vengano fornite informazioni conformi all'Articolo 13 e, ove opportuno, formazione per gli utenti del sistema (deployer)? Sì / No	Importante	
9	Il sistema di gestione dei rischi tiene conto dell'eventuale impatto negativo su persone di età inferiore a 18 anni o altri gruppi vulnerabili?	Importante	
9	I sistemi di IA ad alto rischio sono sottoposti a prove appropriate per individuare le misure di gestione dei rischi più efficaci?	Importante	
9	Le prove sono effettuate in un qualsiasi momento durante l'intero processo di sviluppo e, in ogni caso, prima dell'immissione sul mercato o della messa in servizio del sistema di IA?	Importante	

Dati e governance dei dati - Comprendere e Applicare l'Articolo 10

# Articolo	Domanda	Livello di criticità	Richieste legislatore
10	I set di dati utilizzati per l'addestramento, la convalida e la prova del sistema di IA sono pertinenti, rappresentativi e privi di errori per la finalità prevista del sistema?	Critico	Una risposta negativa indica una non conformità che potrebbe compromettere la sicurezza e i diritti fondamentali
10	Sono in atto pratiche di governance per garantire che i dati raccolti siano pertinenti, corretti e utilizzati per lo scopo dichiarato? I dati sono stati adeguatamente raccolti, annotati, etichettati, puliti e aggiornati?	Critico	*I dati devono essere soggetti a pratiche di governance adeguate, inclusi aspetti come la raccolta, la pulizia,*

			l'annotazione e la sicurezza dei dati
10	È stata effettuata una valutazione delle possibili distorsioni nei dati che potrebbero influire negativamente sulla salute, sicurezza o causare discriminazioni?	Critico	*Deve esserci una valutazione continua delle possibili distorsioni nei dati che potrebbero avere un impatto negativo sui diritti fondamentali o causare discriminazioni.*
10	Sono state adottate misure per prevenire e attenuare le distorsioni identificate?	Critico	*Deve esserci una valutazione continua delle possibili distorsioni nei dati che potrebbero avere un impatto negativo sui diritti fondamentali o causare discriminazioni.*
10	Il sistema tratta dati personali sensibili e, se sì, è strettamente necessario per correggere distorsioni non gestibili con altri dati?	Critico	*Il trattamento di categorie particolari di dati personali deve essere effettuato solo quando strettamente necessario e deve essere soggetto a rigorose misure di protezione.*
10	Sono in atto misure per garantire che i dati sensibili siano protetti da accessi non autorizzati e siano soggetti a rigide limitazioni di riutilizzo?	Critico	*Il trattamento di categorie particolari di dati personali deve essere effettuato solo quando strettamente necessario e deve essere soggetto a rigorose misure di protezione.*
10	I set di dati considerano adeguatamente le caratteristiche specifiche del contesto geografico, comportamentale o funzionale in cui il sistema sarà utilizzato?	Importante	*I set di dati devono avere le proprietà statistiche appropriate e considerare le*

			caratteristiche specifiche del contesto in cui il sistema di IA sarà utilizzato.
10	Sono in atto misure di sicurezza per garantire la protezione dei dati personali utilizzati nel sistema?	Critico	*I dati utilizzati devono essere protetti da misure adeguate per garantirne la sicurezza e la conformità alle normative sulla privacy.*
10	I dati sono adeguatamente pseudonimizzati o resi anonimi quando possibile?	Critico	*I dati utilizzati devono essere protetti da misure adeguate per garantirne la sicurezza e la conformità alle normative sulla privacy.*
10	Esiste una documentazione dettagliata che giustifica il trattamento dei dati personali sensibili e la mancata possibilità di utilizzare dati meno invasivi?	Critico	*È necessario mantenere un registro dettagliato delle attività di trattamento dei dati, inclusi i motivi per cui è stato necessario trattare dati sensibili.*

Documentazione tecnica - Comprendere e Applicare l'Articolo 11

# Articolo	Domanda	Livello di criticità	Richieste legislatore
11	La documentazione tecnica del sistema di IA ad alto rischio è stata redatta prima dell'immissione sul mercato o della messa in servizio?	Critico	*La documentazione tecnica deve essere redatta prima dell'immissione sul mercato o della messa in servizio del sistema e mantenuta aggiornata (Art. 11, Par. 1).*
11	La documentazione tecnica è aggiornata e dimostra che il sistema di IA è conforme ai requisiti del regolamento, fornendo informazioni chiare e comprensibili alle autorità competenti?	Critico	*La documentazione deve dimostrare la conformità del sistema e fornire informazioni necessarie per la valutazione della conformità in modo chiaro e comprensibile (Art. 11, Par. 1).*
11	La documentazione tecnica include tutti gli elementi specificati nell'Allegato IV del regolamento?	Critico	*La documentazione tecnica deve contenere almeno gli elementi di cui all'Allegato IV (Art. 11, Par. 1).*
11	Per le PMI o start-up, la documentazione tecnica è stata fornita utilizzando il modulo di documentazione semplificata definito dalla Commissione Europea?	Importante	*Le PMI possono utilizzare un modulo di documentazione tecnica semplificata fornito dalla Commissione (Art. 11, Par. 1).*
11	Se il sistema di IA è associato a un prodotto regolato dalla normativa di armonizzazione dell'Unione (Allegato I, Sezione A), è stata redatta un'unica documentazione tecnica che comprenda tutte le informazioni richieste?	Critico	*Se un sistema di IA è connesso a un prodotto regolato, deve essere redatta un'unica documentazione tecnica (Art. 11, Par. 2).*

Conversazione delle registrazioni - Comprendere e Applicare l'Articolo 12

# Articolo	Domanda	Livello di criticità	Richieste legislatore
12	Il sistema di IA ad alto rischio consente la registrazione automatica degli eventi ("log") per tutta la durata del ciclo di vita del sistema?	Critico	*I sistemi di IA ad alto rischio devono consentire la registrazione automatica degli eventi per l'intera durata del ciclo di vita del sistema (Art. 12, Par. 1).*
12	Le capacità di registrazione del sistema consentono la registrazione di eventi pertinenti per: a) Individuare situazioni di rischio o modifiche sostanziali? Sì / No Livello di criticità: Critico Riferimento del legislatore: Le registrazioni devono consentire l'individuazione di situazioni di rischio o modifiche sostanziali (Art. 12, Par. 2, Lettera a). b) Facilitare il monitoraggio successivo all'immissione sul mercato? Sì / No Livello di criticità: Importante Riferimento del legislatore: Le registrazioni devono agevolare il monitoraggio successivo all'immissione sul mercato (Art. 12, Par. 2, Lettera b). c) Monitorare il funzionamento del sistema come richiesto dalle normative? Sì / No Livello di criticità: Importante Riferimento del legislatore: Le registrazioni devono permettere il monitoraggio del funzionamento del sistema secondo le normative (Art. 12, Par. 2, Lettera c).	Critico	

12	Per i sistemi di IA specificati nell'Allegato III, le capacità di registrazione includono almeno i dati seguenti: a) Data e ora di inizio e fine di ciascun utilizzo del sistema? Sì / No Livello di criticità: Critico Riferimento del legislatore: Le capacità di registrazione devono comprendere almeno la data e l'ora di inizio e fine di ciascun utilizzo del sistema (Art. 12, Par. 3, Lettera a). b) La banca dati di riferimento utilizzata dal sistema per verificare i dati di input? Sì / No Livello di criticità: Importante Riferimento del legislatore: Le registrazioni devono includere la banca dati di riferimento utilizzata (Art. 12, Par. 3, Lettera b). c) I dati di input per i quali la ricerca ha portato a una corrispondenza? Sì / No Livello di criticità: Importante Riferimento del legislatore: Le registrazioni devono contenere i dati di input che hanno portato a una corrispondenza (Art. 12, Par. 3, Lettera c). d) L'identificativo delle persone fisiche che partecipano alla verifica dei risultati? Sì / No Livello di criticità: Importante Riferimento del legislatore: Devono essere registrati gli identificativi delle persone che partecipano alla verifica dei risultati (Art. 12, Par. 3, Lettera d).	Critico	

Trasparenza e fornitura di informazioni ai deployer - Comprendere e Applicare l'Articolo 13

# Articolo	Domanda	Livello di criticità	Richieste legislatore
13	Il sistema di IA ad alto rischio è progettato per garantire un livello di trasparenza sufficiente affinché i deployer possano interpretare correttamente l'output del sistema e utilizzarlo in modo adeguato?	Critico	*Il sistema deve essere progettato per garantire trasparenza sufficiente per l'uso appropriato da parte dei deployer (Art. 13, Par. 1).*
13	Le istruzioni per l'uso del sistema di IA ad alto rischio includono informazioni concise, complete, corrette e chiare che siano pertinenti, accessibili e comprensibili per i deployer?	Critico	*Il sistema deve essere accompagnato da istruzioni per l'uso comprensibili e accessibili per i deployer (Art. 13, Par. 2).*

13	Le istruzioni per l'uso contengono almeno le informazioni seguenti: a) Identità e dati di contatto del fornitore e del suo rappresentante autorizzato, ove applicabile? Sì / No Livello di criticità: Importante Riferimento del legislatore: Le istruzioni devono includere l'identità e i contatti del fornitore e del suo rappresentante (Art. 13, Par. 3, Lettera a). b) Caratteristiche, capacità e limiti delle prestazioni del sistema di IA, inclusa la finalità prevista e il livello di accuratezza, robustezza e cibersicurezza attesi? Sì / No Livello di criticità: Critico Riferimento del legislatore: Le istruzioni devono dettagliare le caratteristiche, capacità e limiti delle prestazioni del sistema (Art. 13, Par. 3, Lettera b). c) Qualsiasi circostanza nota o prevedibile che possa comportare rischi per la salute, la sicurezza o i diritti fondamentali in caso di uso conforme o improprio del sistema? Sì / No Livello di criticità: Critico	Critico	

Sorveglianza umana - Comprendere e Applicare l'Articolo 14

# Articolo	Domanda	Livello di criticità	Richieste legislatore
14	Il sistema di IA ad alto rischio è progettato e sviluppato per essere supervisionato da persone fisiche durante l'uso, utilizzando strumenti di interfaccia uomo-macchina adeguati?	Critico	*Il sistema deve essere progettato per consentire una sorveglianza umana efficace durante il periodo di utilizzo (Art. 14, Par. 1).*
14	Le misure di sorveglianza umana adottate mirano a prevenire o ridurre al minimo i rischi per la salute, la sicurezza o i diritti fondamentali, considerando sia l'uso previsto sia l'uso improprio ragionevolmente prevedibile?	Critico	*Le misure devono essere adeguate per minimizzare i rischi residui nonostante l'applicazione di altri requisiti (Art. 14, Par. 2).*
14	Le misure di sorveglianza umana sono commisurate ai rischi, al livello di autonomia e al contesto di utilizzo del sistema di IA?	Importante	*Le misure devono essere proporzionate ai rischi e al contesto d'uso del sistema (Art. 14, Par. 3).*
14	Le misure di sorveglianza umana includono almeno una delle seguenti tipologie: a) Misure integrate nel sistema di IA dal fornitore prima della sua immissione sul mercato? Sì / No Livello di criticità: Importante Riferimento del legislatore: Misure integrate nel sistema dal fornitore (Art. 14, Par. 3, Lettera a). b) Misure attuabili dal deployer, individuate dal fornitore prima dell'immissione sul mercato? Sì / No Livello di criticità: Importante Riferimento del legislatore: Misure attuabili dal deployer (Art. 14, Par. 3, Lettera b).	Importante	

14	Il sistema di IA è fornito al deployer in modo tale che le persone incaricate della sorveglianza umana possano: a) Comprendere correttamente le capacità e i limiti del sistema e monitorarne il funzionamento per individuare anomalie, disfunzioni e prestazioni inattese? Sì / No Livello di criticità: Critico Riferimento del legislatore: Le persone incaricate della sorveglianza devono comprendere le capacità e i limiti del sistema (Art. 14, Par. 4, Lettera a). b) Restare consapevoli della possibile distorsione dell'automazione e del rischio di fare eccessivo affidamento sull'output del sistema? Sì / No Livello di criticità: Importante Riferimento del legislatore: Deve essere garantita la consapevolezza della distorsione dell'automazione (Art. 14, Par. 4, Lettera b). c) Interpretare correttamente l'output del sistema, utilizzando strumenti e metodi di interpretazione disponibili? Sì / No Livello di criticità: Critico Riferimento del legislatore: Il sistema deve consentire l'interpretazione corretta degli output (Art. 14, Par. 4, Lettera c). d) Decidere di non utilizzare il sistema o ignorarne, annullarne o ribaltarne l'output in situazioni particolari? Sì / No Livello di criticità: Critico Riferimento del legislatore: Il sistema deve consentire di non utilizzare o ignorare l'output (Art. 14, Par. 4, Lettera d). e) Intervenire sul funzionamento del sistema o interromperlo mediante un pulsante di "arresto" o procedura analoga? Sì / No Livello di criticità: Critico Riferimento del legislatore: Deve essere possibile interrompere il funzionamento del sistema in sicurezza (Art. 14, Par. 4, Lettera e).	Critico	

14	Per i sistemi di IA di cui all'Allegato III, le misure adottate garantiscono che il deployer non compia azioni o adotti decisioni basate sull'identificazione risultante dal sistema, a meno che l'identificazione non sia stata verificata separatamente da almeno due persone competenti?	Critico	*L'identificazione deve essere verificata separatamente da almeno due persone competenti, salvo eccezioni specifiche (Art. 14, Par. 5).*

Accuratezza, robustezza e cibersicurezza - Comprendere e Applicare l'Articolo 15

# Articolo	Domanda	Livello di criticità	Richieste legislatore
15	Il sistema di IA ad alto rischio è progettato per raggiungere un livello adeguato di accuratezza, robustezza e cibersicurezza durante tutto il ciclo di vita?	Critico	*Il sistema deve operare in modo coerente con livelli adeguati di accuratezza, robustezza e cibersicurezza (Art. 15, Par. 1).*
15	I livelli di accuratezza e le metriche pertinenti sono dichiarati nelle istruzioni per l'uso che accompagnano il sistema di IA?	Importante	*I livelli di accuratezza e le metriche pertinenti devono essere dichiarati nelle istruzioni per l'uso (Art. 15, Par. 3).*
15	Il sistema di IA ad alto rischio è resiliente a errori, guasti o incongruenze che possono verificarsi all'interno del sistema o nell'ambiente operativo?	Critico	*Il sistema deve essere il più resiliente possibile ai guasti o errori (Art. 15, Par. 4).*
15	Il sistema di IA ad alto rischio è progettato per prevenire, accertare, rispondere, risolvere e controllare attacchi, compresi data poisoning, model poisoning, evasione del modello e attacchi alla riservatezza?	Critico	*Devono essere adottate misure tecniche per affrontare le vulnerabilità specifiche dell'IA (Art. 15, Par. 5).*

Obblighi dei fornitori dei sistemi di IA ad alto rischio - Comprendere e Applicare l'Articolo 16

# Articolo	Domanda	Livello di criticità	Richieste legislatore
16	Il fornitore garantisce che i sistemi di IA ad alto rischio siano conformi ai requisiti di cui alla Sezione 2?	Critico	*I fornitori devono garantire la conformità ai requisiti della Sezione 2 (Art. 16, Lettera a).*
16	Il nome, la denominazione commerciale registrata, il marchio registrato del fornitore e l'indirizzo di contatto sono indicati sul sistema di IA, sul suo imballaggio o sui documenti di accompagnamento?	Critico	*Il fornitore deve indicare queste informazioni sul sistema, imballaggio o documenti di accompagnamento (Art. 16, Lettera b).*
16	Il fornitore dispone di un sistema di gestione della qualità conforme all'Articolo 17?	Critico	*I fornitori devono avere un sistema di gestione della qualità conforme (Art. 16, Lettera c).*
16	Il fornitore conserva la documentazione tecnica relativa al sistema di IA ad alto rischio come specificato nell'Articolo 18?	Critico	*I fornitori devono conservare la documentazione tecnica (Art. 16, Lettera d).*
16	Il fornitore conserva i log generati automaticamente dai sistemi di IA ad alto rischio quando sono sotto il suo controllo, come previsto dall'Articolo 19?	Critico	*I fornitori devono conservare i log generati automaticamente (Art. 16, Lettera e).*
16	Il sistema di IA ad alto rischio è stato sottoposto alla procedura di valutazione della conformità pertinente prima di essere immesso sul mercato o messo in servizio, come richiesto dall'Articolo 43?	Critico	*I fornitori devono garantire che il sistema sia sottoposto alla valutazione di conformità (Art. 16, Lettera f).*
16	Il fornitore ha elaborato una dichiarazione di conformità UE in conformità con l'Articolo 47?	Importante	*I fornitori devono elaborare una dichiarazione di conformità UE*

			(Art. 16, Lettera g).
16	Il fornitore ha apposto la marcatura CE sul sistema di IA ad alto rischio, oppure, ove ciò non sia possibile, sul suo imballaggio o sui documenti di accompagnamento, per indicare la conformità al regolamento, come previsto dall'Articolo 48?	Critico	*I fornitori devono apporre la marcatura CE per indicare la conformità al regolamento (Art. 16, Lettera h).*
16	Il fornitore rispetta gli obblighi di registrazione di cui all'Articolo 49, paragrafo 1?	Importante	*I fornitori devono rispettare gli obblighi di registrazione (Art. 16, Lettera i).*
16	Il fornitore adotta le necessarie misure correttive e fornisce le informazioni necessarie in conformità con l'Articolo 20?	Critico	*I fornitori devono adottare le misure correttive necessarie e fornire informazioni (Art. 16, Lettera j).*
16	Su richiesta motivata di un'autorità nazionale competente, il fornitore può dimostrare la conformità del sistema di IA ad alto rischio ai requisiti della Sezione 2?	Importante	*I fornitori devono essere in grado di dimostrare la conformità ai requisiti (Art. 16, Lettera k).*
16	Il sistema di IA ad alto rischio è conforme ai requisiti di accessibilità in conformità con le direttive (UE) 2016/2102 e (UE) 2019/882?	Importante	*I fornitori devono garantire la conformità ai requisiti di accessibilità (Art. 16, Lettera l).*

Obblighi dei fornitori dei sistemi di IA ad alto rischio - Comprendere e Applicare l'Articolo 17

# Articolo	Domanda	Livello di criticità	Richieste legislatore
17	Il fornitore ha istituito un sistema di gestione della qualità che garantisce la conformità al regolamento?	Critico	*I fornitori devono avere un sistema di gestione della qualità che garantisca la conformità al regolamento (Art. 17, Par. 1).*
17	Il sistema di gestione della qualità documenta in modo sistematico e ordinato sotto forma di politiche, procedure e istruzioni scritte?	Importante	*Il sistema deve essere documentato in modo sistematico e ordinato (Art. 17, Par. 1).*
17	Il sistema di gestione della qualità include una strategia per la conformità normativa, comprese le procedure di valutazione della conformità e di gestione delle modifiche ai sistemi di IA ad alto rischio?	Critico	*Deve essere inclusa una strategia per la conformità normativa (Art. 17, Par. 1, Lettera a).*
17	Il sistema prevede tecniche, procedure e interventi sistematici per la progettazione, il controllo e la verifica della progettazione del sistema di IA ad alto rischio?	Importante	*Deve includere tecniche, procedure e interventi per la progettazione e la verifica del sistema (Art. 17, Par. 1, Lettera b).*
17	Il sistema di gestione della qualità comprende tecniche, procedure e interventi sistematici per lo sviluppo e per il controllo e la garanzia della qualità del sistema di IA ad alto rischio?	Critico	*Devono essere presenti procedure per lo sviluppo e la garanzia della qualità (Art. 17, Par. 1, Lettera c).*
17	Il sistema prevede procedure di esame, prova e convalida da effettuare prima, durante e dopo lo sviluppo del sistema di IA, e specifica la frequenza con cui devono essere effettuate?	Importante	*Devono essere definite procedure di esame, prova e convalida (Art. 17, Par. 1, Lettera d).*
17	Il sistema di gestione della qualità specifica le norme tecniche da applicare e, ove le norme armonizzate non siano pienamente applicate, i mezzi per garantire la conformità ai requisiti della sezione 2?	Importante	*Devono essere specificate le norme tecniche e i mezzi per garantire la conformità (Art. 17, Par. 1, Lettera e).*
17	Il sistema comprende sistemi e procedure per la gestione dei dati, inclusa l'acquisizione, raccolta, analisi, etichettatura, archiviazione, filtrazione, estrazione, aggregazione e conservazione dei dati?	Critico	*Devono essere inclusi sistemi e procedure per la gestione dei dati (Art. 17, Par. 1, Lettera f).*

17	Il sistema di gestione della qualità include il sistema di gestione dei rischi conforme all'Articolo 9?	Critico	*Deve includere il sistema di gestione dei rischi (Art. 17, Par. 1, Lettera g).*
17	Il sistema prevede un sistema di monitoraggio successivo all'immissione sul mercato conforme all'Articolo 72?	Importante	*Deve essere previsto un sistema di monitoraggio successivo all'immissione sul mercato (Art. 17, Par. 1, Lettera h).*
17	Il sistema include procedure per la segnalazione di incidenti gravi come previsto dall'Articolo 73?	Importante	*Devono essere incluse procedure per la segnalazione di incidenti gravi (Art. 17, Par. 1, Lettera i).*
17	Il sistema prevede la gestione della comunicazione con le autorità nazionali competenti, altre autorità pertinenti, organismi notificati, operatori, clienti o altre parti interessate?	Importante	*Deve esserci un sistema per la gestione della comunicazione con le autorità e le parti interessate (Art. 17, Par. 1, Lettera j).*
17	Il sistema include procedure per la conservazione delle registrazioni e di tutte le informazioni e documentazioni pertinenti?	Importante	*Devono essere previste procedure per la conservazione delle registrazioni (Art. 17, Par. 1, Lettera k).*
17	Il sistema di gestione della qualità include la gestione delle risorse, comprese le misure relative alla sicurezza dell'approvvigionamento?	Importante	*Deve essere prevista la gestione delle risorse, inclusa la sicurezza dell'approvvigionamento (Art. 17, Par. 1, Lettera l).*
17	Il sistema definisce un quadro di responsabilità per la dirigenza e il personale in relazione a tutti gli aspetti elencati nel regolamento?	Importante	*Deve esserci un quadro di responsabilità per la dirigenza e il personale (Art. 17, Par. 1, Lettera m).*
17	Il sistema di gestione della qualità è proporzionato alle dimensioni dell'organizzazione del fornitore e mantiene il rigore e il livello di protezione necessari per garantire la conformità?	Importante	*L'attuazione deve essere proporzionata alle dimensioni dell'organizzazione, mantenendo il rigore necessario (Art. 17, Par. 2).*
17	Per i fornitori soggetti a obblighi relativi a sistemi di gestione della qualità a norma del diritto dell'Unione, gli aspetti elencati al paragrafo 1 sono inclusi nel sistema di gestione della qualità esistente?	Importante	*Gli aspetti devono essere inclusi nei sistemi di gestione della qualità esistenti (Art. 17, Par. 3).*

17	Per i fornitori che sono istituti finanziari, il sistema di gestione della qualità soddisfa i requisiti in materia di governance e processi interni stabiliti dal diritto dell'Unione in materia di servizi finanziari?	Importante	*Gli istituti finanziari devono soddisfare i requisiti di governance e processi interni stabiliti dal diritto dell'Unione (Art. 17, Par. 4).*

Conservazione dei documenti - Comprendere e Applicare l'Articolo 18

# Articolo	Domanda	Livello di criticità	Richieste legislatore
18	Il fornitore conserva la documentazione tecnica di cui all'Articolo 11 per un periodo di 10 anni dopo che il sistema di IA ad alto rischio è stato immesso sul mercato o messo in servizio?	Critico	*Il fornitore deve conservare la documentazione tecnica per 10 anni (Art. 18, Par. 1, Lettera a).*
18	Il fornitore conserva la documentazione relativa al sistema di gestione della qualità di cui all'Articolo 17 per il periodo specificato?	Importante	*Il fornitore deve conservare la documentazione relativa al sistema di gestione della qualità (Art. 18, Par. 1, Lettera b).*
18	Il fornitore conserva la documentazione relativa alle modifiche approvate dagli organismi notificati e le decisioni rilasciate dagli organismi notificati, ove applicabile?	Importante	*Il fornitore deve conservare la documentazione relativa alle modifiche e le decisioni degli organismi notificati (Art. 18, Par. 1, Lettere c e d).*
18	Il fornitore conserva la dichiarazione di conformità UE di cui all'Articolo 47 per il periodo indicato?	Importante	*Il fornitore deve conservare la dichiarazione di conformità UE per 10 anni (Art. 18, Par. 1, Lettera e).*
18	Il fornitore ha stabilito le condizioni per garantire che la documentazione resti a disposizione delle autorità nazionali competenti nel caso in cui fallisca o cessi la sua attività prima della fine del periodo di conservazione?	Importante	*Le condizioni per la conservazione della documentazione devono essere stabilite in caso di cessazione dell'attività (Art. 18, Par. 2).*

Log generati automaticamente - Comprendere e Applicare l'Articolo 19

# Articolo	Domanda	Livello di criticità	Richieste legislatore
19	Il fornitore conserva i log generati automaticamente dai sistemi di IA ad alto rischio nella misura in cui sono sotto il suo controllo, per un periodo adeguato alla finalità prevista, di almeno sei mesi?	Critico	*I log devono essere conservati per almeno sei mesi o secondo il diritto applicabile (Art. 19, Par. 1).*

Misure correttive e dovere di informazione - Comprendere e Applicare l'Articolo 20

Misure attive correttive in caso di incidenti/non compliance dei fornitori/problemi:

# Articolo	Domanda	Livello di criticità	Richieste legislatore
20	Il fornitore adotta immediatamente le misure correttive necessarie (rendere conforme, ritirare, disabilitare o richiamare il sistema) se ritiene che un sistema di IA ad alto rischio non sia conforme al regolamento?	Critico	*Il fornitore deve adottare misure correttive immediatamente in caso di non conformità (Art. 20, Par. 1).*
20	Il fornitore indaga immediatamente sulle cause del rischio e informa le autorità competenti se un sistema di IA ad alto rischio presenta un rischio ai sensi dell'Articolo 79, Paragrafo 1?	Critico	*Il fornitore deve indagare e informare le autorità competenti in caso di rischio (Art. 20, Par. 2).*

Cooperazione con le Autorità Competenti - Comprendere e Applicare l'Articolo 21

# Articolo	Domanda	Livello di criticità	Richieste legislatore
21	Il fornitore fornisce, su richiesta motivata di un'autorità competente, tutte le informazioni e la documentazione necessarie per dimostrare la conformità del sistema di IA ad alto rischio ai requisiti della Sezione 2?	Importante	*Il fornitore deve fornire tutte le informazioni richieste per dimostrare la conformità (Art. 21, Par. 1).*
21	Il fornitore concede all'autorità competente l'accesso ai log generati automaticamente, ove richiesto e nella misura in cui sono sotto il suo controllo?	Importante	*Il fornitore deve consentire l'accesso ai log generati automaticamente (Art. 21, Par. 2).*

Rappresentanti Autorizzati dei Fornitori - Comprendere e Applicare l'Articolo 22

# Articolo	Domanda	Livello di criticità	Richieste legislatore
22	Se il fornitore è stabilito in un paese terzo, ha nominato un rappresentante autorizzato nell'Unione mediante mandato scritto?	Critico	*I fornitori stabiliti in paesi terzi devono nominare un rappresentante autorizzato nell'Unione (Art. 22, Par. 1).*
22	Il rappresentante autorizzato esegue i compiti specificati nel mandato ricevuto dal fornitore e fornisce una copia del mandato alle autorità di vigilanza del mercato su richiesta?	Importante	*Il rappresentante autorizzato deve eseguire i compiti specificati nel mandato e fornire una copia su richiesta (Art. 22, Par. 3).*
22	Il rappresentante autorizzato verifica che la dichiarazione di conformità UE e la documentazione tecnica siano state redatte e che il fornitore abbia eseguito un'appropriata procedura di valutazione della conformità?	Critico	*Il rappresentante autorizzato deve verificare la conformità della documentazione e delle procedure (Art. 22, Par. 3, Lettera a).*
22	Il rappresentante autorizzato tiene a disposizione delle autorità competenti i contatti del fornitore, la dichiarazione di conformità UE, la documentazione tecnica e, se del caso, il certificato rilasciato dall'organismo notificato per 10 anni?	Importante	*Il rappresentante autorizzato deve mantenere la documentazione disponibile per 10 anni (Art. 22, Par. 3, Lettera b).*
22	Il rappresentante autorizzato fornisce, su richiesta, tutte le informazioni necessarie per dimostrare la conformità del sistema di IA ad alto rischio ai requisiti, compreso l'accesso ai log generati automaticamente?	Importante	*Il rappresentante autorizzato deve fornire tutte le informazioni necessarie per dimostrare la conformità (Art. 22, Par. 3, Lettera c).*
22	Il rappresentante autorizzato coopera con le autorità competenti su richiesta motivata riguardo	Importante	*Il rappresentante autorizzato deve cooperare con le*

	a qualsiasi azione intrapresa in relazione al sistema di IA ad alto rischio?		*autorità competenti (Art. 22, Par. 3, Lettera d).*
22	Il rappresentante autorizzato rispetta gli obblighi di registrazione di cui all'Articolo 49, Paragrafo 1, o garantisce la correttezza delle informazioni se la registrazione è effettuata dal fornitore?	Importante	*Il rappresentante autorizzato deve rispettare gli obblighi di registrazione o garantire la correttezza delle informazioni (Art. 22, Par. 3, Lettera e).*
22	Il rappresentante autorizzato interrompe il mandato se ritiene che il fornitore stia violando i suoi obblighi e comunica immediatamente la cessazione del mandato all'autorità di vigilanza del mercato?	Critico	*Il rappresentante autorizzato deve interrompere il mandato e comunicare alle autorità in caso di violazione degli obblighi (Art. 22, Par. 4).*

Obblighi degli Importatori - Comprendere e Applicare l'Articolo 23

# Articolo	Domanda	Livello di criticità	Richieste legislatore
23	L'importatore ha verificato che il fornitore del sistema di IA ad alto rischio abbia eseguito la procedura di valutazione della conformità pertinente?	Critico	*L'importatore deve garantire che il fornitore abbia eseguito la procedura di valutazione della conformità del decreto AI ACT (Art. 23, Par. 1, Lettera a).*
23	L'importatore verifica che il fornitore abbia redatto la documentazione tecnica conformemente all'Articolo 11 e all'Allegato IV?	Importante	*L'importatore deve verificare la presenza della documentazione tecnica (Art. 23, Par. 1, Lettera b).*
23	L'importatore ha verificato che il sistema di IA ad alto rischio rechi la marcatura CE e sia accompagnato dalla dichiarazione di conformità UE e dalle istruzioni per l'uso?	Critico	*L'importatore deve verificare la marcatura CE e la presenza della dichiarazione di conformità UE (Art. 23, Par. 1, Lettera c).*
23	L'importatore ha verificato che il fornitore abbia nominato un rappresentante autorizzato nell'Unione Europea?	Importante	*Il fornitore deve aver nominato un rappresentante autorizzato (Art. 23, Par. 1, Lettera d).*
23	L'importatore si astiene dall'immettere sul mercato un sistema di IA ad alto rischio se ha motivo di ritenere che non sia conforme al regolamento, o che sia falsificato o accompagnato da documentazione falsificata?	Critico	*L'importatore deve astenersi dall'immettere sul mercato sistemi non conformi o falsificati (Art. 23, Par. 2).*
23	L'importatore indica il proprio nome, denominazione commerciale registrata o marchio e l'indirizzo di contatto sul sistema di IA ad alto rischio e sul suo imballaggio o in un documento di accompagnamento, ove applicabile?	Importante	*L'importatore deve fornire le proprie informazioni di contatto (Art. 23, Par. 3).*

23	L'importatore garantisce che le condizioni di stoccaggio o di trasporto non pregiudichino la conformità del sistema di IA ad alto rischio ai requisiti del regolamento?	Importante	*L'importatore deve garantire che le condizioni di stoccaggio e trasporto non pregiudichino la conformità (Art. 23, Par. 4).*
23	L'importatore conserva una copia del certificato rilasciato dall'organismo notificato, le istruzioni per l'uso e la dichiarazione di conformità UE per 10 anni dalla data di immissione sul mercato del sistema di IA ad alto rischio?	Importante	*Certificato rilasciato dall'organismo notificato: Se un sistema di IA ad alto rischio richiede una valutazione da parte di un organismo notificato (cioè un ente indipendente autorizzato a verificare la conformità del sistema ai requisiti del regolamento), l'importatore deve conservare una copia del certificato che attesta la conformità del sistema.* *Istruzioni per l'uso: Devono essere conservate le istruzioni per l'uso del sistema di IA ad alto rischio, che devono includere informazioni chiare e complete su come utilizzare correttamente il sistema, quali sono le sue capacità e limiti, e come gestire eventuali rischi o problemi operativi.*

			Dichiarazione di conformità UE: Questa dichiarazione è un documento formale che attesta che il sistema di IA ad alto rischio è conforme ai requisiti previsti dal regolamento dell'UE. Il fornitore del sistema deve redigere questa dichiarazione secondo quanto specificato all'articolo 47.
23	L'importatore conserva una copia del certificato rilasciato dall'organismo notificato, le istruzioni per l'uso e la dichiarazione di conformità UE per 10 anni dalla data di immissione sul mercato del sistema di IA ad alto rischio?	Critico	*L'importatore deve conservare la documentazione per 10 anni (Art. 23, Par. 5).*
23	L'importatore può fornire su richiesta motivata delle autorità competenti tutte le informazioni e la documentazione necessarie per dimostrare la conformità del sistema di IA ad alto rischio?	Importante	*L'importatore deve fornire la documentazione alle autorità competenti su richiesta (Art. 23, Par. 6).*
23	L'importatore coopera con le autorità competenti in qualsiasi azione intrapresa in relazione a un sistema di IA ad alto rischio immesso sul mercato?	Importante	*L'importatore deve cooperare con le autorità competenti (Art. 23, Par. 7).*

Obblighi dei Distributori - Comprendere e Applicare l'Articolo 24

# Articolo	Domanda	Livello di criticità	Richieste legislatore
24	Prima di immettere sul mercato il prodotto il distributore verifica che il sistema di IA ad alto rischio rechi la marcatura CE e sia accompagnato dalla dichiarazione di conformità UE e dalle istruzioni per l'uso?	Critico	*Il distributore deve verificare la marcatura CE e la presenza della dichiarazione di conformità UE (Art. 24, Par. 1).*
24	Il distributore garantisce che il fornitore e l'importatore del sistema di IA ad alto rischio abbiano rispettato i loro rispettivi obblighi?	Importante	*Il distributore deve garantire il rispetto degli obblighi da parte del fornitore e dell'importatore (Art. 24, Par. 1).*
24	Il distributore si astiene dal mettere a disposizione sul mercato un sistema di IA ad alto rischio se ritiene che non sia conforme al regolamento?	Critico	*Il distributore deve astenersi dal mettere a disposizione sistemi non conformi (Art. 24, Par. 2).*
24	Il distributore garantisce che le condizioni di stoccaggio o di trasporto del sistema di IA ad alto rischio sotto la sua responsabilità non pregiudichino la conformità ai requisiti del regolamento?	Importante	*Il distributore deve garantire che le condizioni di stoccaggio e trasporto non pregiudichino la conformità (Art. 24, Par. 3).*
24	Il distributore adotta le misure correttive necessarie se ritiene che un sistema di IA ad alto rischio non sia conforme ai requisiti del regolamento?	Critico	*Il distributore deve adottare misure correttive per rendere il sistema conforme (Art. 24, Par. 4).*
24	Il distributore può fornire alle autorità competenti, su richiesta, tutte le informazioni e la documentazione necessarie per dimostrare la conformità del sistema di IA ad alto rischio?	Importante	*Il distributore deve fornire informazioni alle autorità competenti su richiesta (Art. 24, Par. 5).*
24	Il distributore coopera con le autorità competenti in qualsiasi azione intrapresa in relazione a un sistema di IA ad alto rischio messo a disposizione sul mercato?	Importante	*Il distributore deve cooperare con le autorità competenti (Art. 24, Par. 6).*

Responsabilità lungo la catena del valore dell'IA - Comprendere e Applicare l'Articolo 25

# Articolo	Domanda	Livello di criticità	Richieste legislatore
25	Il distributore, importatore, deployer o altro terzo ha apposto il proprio nome o marchio su un sistema di IA ad alto rischio già immesso sul mercato o messo in servizio?	Importante	*Se si, è considerato fornitore se appone il proprio nome o marchio su un sistema già immesso sul mercato (Art. 25, Par. 1, Lettera a).*
25	Il distributore, importatore, deployer o altro terzo ha apportato una modifica sostanziale a un sistema di IA ad alto rischio già immesso sul mercato?	Critico	*Se si, è considerato fornitore se appone il proprio nome o marchio su un sistema già immesso sul mercato (Art. 25, Par. 1, Lettera a).*
25	Il distributore, importatore, deployer o altro terzo ha modificato la finalità prevista di un sistema di IA, rendendolo un sistema di IA ad alto rischio?	Critico	*Considerato fornitore se modifica la finalità prevista del sistema rendendolo ad alto rischio (Art. 25, Par. 1, Lettera c).*
25	Nel caso in cui il fornitore iniziale non sia più considerato fornitore, ha fornito l'accesso tecnico, le informazioni e l'assistenza necessari al nuovo fornitore?	Importante	*Il fornitore iniziale deve cooperare con il nuovo fornitore per garantire la conformità (Art. 25, Par. 2).*
25	Il fabbricante del prodotto che contiene un sistema di IA ad alto rischio come componente di sicurezza è identificato come fornitore del sistema di IA nelle seguenti circostanze: Il sistema di IA ad alto rischio è stato immesso sul mercato insieme al prodotto con il nome o il marchio del fabbricante del prodotto? Il sistema di IA ad alto rischio è stato messo in servizio con il nome o il marchio del fabbricante del prodotto dopo che il prodotto è stato immesso sul mercato?	Critico	*Il fabbricante del prodotto è considerato fornitore del sistema di IA ad alto rischio se soddisfa una delle condizioni specificate (Art. 25, Par. 3, Lettere a e b).* ***Risposta "No"****: Indica una possibile non conformità riguardo al riconoscimento del fabbricante come fornitore del sistema di IA ad alto rischio, e potrebbe richiedere un'ulteriore verifica*

			delle responsabilità legali. ***Risposta "Sì"**: Indica che il fabbricante è correttamente riconosciuto come fornitore e deve rispettare gli obblighi dell'Articolo 16.*

Obblighi dei deployer dei sistemi di IA ad alto rischio - Comprendere e Applicare l'Articolo 26

# Articolo	Domanda	Livello di criticità	Richieste legislatore
26	Il deployer adotta misure tecniche e organizzative per garantire che i sistemi di IA ad alto rischio siano utilizzati conformemente alle istruzioni per l'uso?	Critico	*I deployer devono utilizzare i sistemi di IA secondo le istruzioni per l'uso (Art. 26, Par. 1).*
26	Il deployer affida la sorveglianza umana del sistema di IA ad alto rischio a persone fisiche competenti, formate e con l'autorità necessaria?	Importante	*La sorveglianza umana deve essere affidata a personale competente (Art. 26, Par. 2).*
26	Il deployer garantisce che i dati di input utilizzati dal sistema di IA ad alto rischio siano pertinenti e sufficientemente rappresentativi della finalità prevista del sistema?	Critico	*I dati di input devono essere pertinenti e rappresentativi (Art. 26, Par. 4).*
26	Il deployer monitora il funzionamento del sistema di IA ad alto rischio e informa i fornitori o le autorità competenti in caso di rilevazione di rischi o incidenti gravi?	Critico	*Deployer devono monitorare il sistema e informare in caso di rischi (Art. 26, Par. 5).*
26	I deployer conservano log generati automaticamente dal sistema di IA ad alto rischio per almeno sei mesi o per un periodo adeguato alla finalità del sistema?	Importante	*I log devono essere conservati per almeno sei mesi o per il periodo richiesto (Art. 26, Par. 6).*

26	I deployer informano i rappresentanti dei lavoratori e i lavoratori interessati prima di mettere in servizio o utilizzare un sistema di IA ad alto rischio sul luogo di lavoro?	Importante	*I lavoratori devono essere informati sull'uso dei sistemi di IA ad alto rischio (Art. 26, Par. 7).*
26	I deployer verificano che il sistema di IA ad alto rischio che intendete utilizzare sia stato registrato nella banca dati dell'UE, ove richiesto, e, in caso contrario, informate il fornitore o il distributore?	Importante	*Deployer devono verificare la registrazione del sistema di IA (Art. 26, Par. 8).*
26	I deployer utilizzano le informazioni fornite a norma dell'articolo 13 per adempiere all'obbligo di effettuare una valutazione d'impatto sulla protezione dei dati, se del caso?	Importante	*Le informazioni devono essere utilizzate per valutare l'impatto sulla protezione dei dati (Art. 26, Par. 9).*
26	I deployer hanno richiesto un'autorizzazione ex ante o entro 48 ore per l'uso di sistemi di identificazione biometrica remota a posteriori, se richiesto?	Critico	*Deployer devono ottenere un'autorizzazione per l'uso di sistemi di identificazione biometrica remota a posteriori (Art. 26, Par. 10).*
26	I deployer hanno informato le persone fisiche che sono soggette all'uso del sistema di IA ad alto rischio, ove richiesto?	Importante	*Le persone fisiche devono essere informate sull'uso del sistema di IA (Art. 26, Par. 11).*
26	I deployer cooperano con le autorità competenti in merito a qualsiasi azione intrapresa in relazione al sistema di IA ad alto rischio?	Importante	*I deployer devono cooperare con le autorità competenti (Art. 26, Par. 12): I deployer cooperano con le pertinenti autorità competenti in merito a qualsiasi azione intrapresa da dette autorità in relazione al sistema di IA ad*

			alto rischio ai fini dell'attuazione del presente regolamento.

Valutazione d'impatto sui diritti fondamentali per i sistemi di IA ad alto rischio - Comprendere e Applicare l'Articolo 27

# Articolo	Domanda	Livello di criticità	Richieste legislatore
27	Il deployer ha effettuato una valutazione d'impatto sui diritti fondamentali prima di utilizzare un sistema di IA ad alto rischio?	Critico	*Art. 27, Par. 1 - Prima di utilizzare un sistema di IA ad alto rischio, i deployer devono effettuare una valutazione dell'impatto sui diritti fondamentali.*
27	La valutazione del deployer include i seguenti elementi: a) Una descrizione dei processi in cui verrà utilizzato il sistema di IA? b) Una descrizione del periodo e della frequenza di utilizzo del sistema di IA? c) Le categorie di persone fisiche o gruppi che potrebbero essere interessati dall'uso del sistema di IA? d) I rischi specifici di danno che potrebbero incidere su tali categorie di persone fisiche o gruppi? e) Le misure di sorveglianza umana attuate secondo le istruzioni per l'uso? f) Le misure da adottare qualora i rischi si concretizzino, incluse disposizioni di governance interna e meccanismi di reclamo?	Critico	*Art. 27, Par. 1 - La valutazione deve includere una serie di elementi specifici come descritti nel paragrafo 1, lettere a) - f).*

27	Il deployer una volta effettuata una valutazione d'impatto sulla protezione dei dati (DPIA) ai sensi del Regolamento (UE) 2016/679, ha integrato tale valutazione con la valutazione d'impatto sui diritti fondamentali?	Importante	*Art. 27, Par. 4 - La valutazione d'impatto sui diritti fondamentali deve integrare la DPIA se già effettuata.*
27	Il deployer ha notificato i risultati della valutazione d'impatto sui diritti fondamentali all'autorità di vigilanza del mercato?	Critico	*Art. 27, Par. 3 - Il deployer deve notificare i risultati della valutazione all'autorità di vigilanza del mercato, presentando il modello compilato di cui al paragrafo 5 del presente articolo nell'ambito della notifica*
27	Nel caso di cambiamenti o aggiornamenti durante l'uso del sistema di IA ad alto rischio, il deployer ha provveduto ad aggiornare la valutazione d'impatto sui diritti fondamentali?	Importante	*Art. 27, Par. 2 - I deployer devono aggiornare la valutazione se qualsiasi elemento considerato cambia o non è più aggiornato.*
27	Il deployer utilizza il modello di questionario fornito dall'ufficio per l'IA per la valutazione d'impatto sui diritti fondamentali?	Critico	*Art. 27, Par. 5 - L'ufficio per l'IA fornisce un modello di questionario per agevolare la valutazione d'impatto.*

Presunzione di conformità a determinati requisiti - Comprendere e Applicare l'Articolo 42

# Articolo	Domanda	Livello di criticità	Richieste legislatore
42	I vostri sistemi di IA ad alto rischio sono stati addestrati e sottoposti a prova con dati che rispecchiano il contesto geografico, comportamentale, contestuale o funzionale specifico per il loro utilizzo previsto?	Critico	*Art. 42, Par. 1 - I sistemi di IA addestrati e testati in contesti specifici si presumono conformi ai requisiti di cui all'Articolo 10, Paragrafo 4.*
42	I vostri sistemi di IA ad alto rischio sono stati certificati o hanno una dichiarazione di conformità nell'ambito di un sistema di cibersicurezza a norma del regolamento (UE) 2019/881?	Critico	*Art. 42, Par. 2 - I sistemi certificati secondo il regolamento UE 2019/881 si presumono conformi ai requisiti di cibersicurezza di cui all'Articolo 15.*
42	I riferimenti per la certificazione o la dichiarazione di conformità del vostro sistema di IA ad alto rischio sono stati pubblicati nella Gazzetta ufficiale dell'Unione europea?	Importante	*Art. 42, Par. 2 - La pubblicazione dei riferimenti nella Gazzetta ufficiale UE conferma la presunzione di conformità ai requisiti di cibersicurezza.*

Valutazione della conformità - Comprendere e Applicare l'Articolo 43

Queste domande sono progettate per verificare che il fornitore di sistemi di IA ad alto rischio abbia seguito le procedure di valutazione della conformità appropriate e soddisfi i requisiti previsti dall'Articolo 43 del regolamento.

# Articolo	Domanda	Livello di criticità	Richieste legislatore
43	Il fornitore ha seguito una procedura di valutazione della conformità basata sul controllo interno o sulla valutazione del sistema di gestione della qualità per i sistemi di IA ad alto rischio elencati nell'Allegato III, punto 1? Opzioni: a) Controllo interno (Allegato VI) b) Valutazione del sistema di gestione della qualità e documentazione tecnica (Allegato VII)	Critico	*Art. 43, Par. 1*
43	Il fornitore,ha seguito la procedura di valutazione della conformità di cui all'Allegato VII se: a) non esistono le norme armonizzate di cui all'articolo 40 e non sono disponibili le specifiche comuni di cui all'articolo 41; b) il fornitore non ha applicato la norma armonizzata o ne ha applicato solo una parte; c) esistono le specifiche comuni di cui alla lettera a), ma il fornitore non le ha applicate; d) una o più norme armonizzate di cui alla lettera a) sono state pubblicate con una limitazione e soltanto sulla parte della norma che è oggetto di limitazione	Critico	*Art. 43, Par. 1*
43	Il fornitore ha utilizzato un organismo notificato per la valutazione della conformità, se il sistema di IA ad alto rischio è destinato ad essere messo in servizio da autorità competenti in materia di contrasto, immigrazione o asilo?	Importante	*Art. 43, Par. 1*
43	Il fornitore ha seguito la procedura di valutazione della conformità basata sul controllo interno per i sistemi di IA ad alto rischio di cui all'Allegato III, punti da 2 a 8?	Importante	*Art. 43, Par. 2*
43	Il fornitore ha sottoposto il sistema di IA ad alto rischio a una nuova procedura di valutazione della conformità in caso di una modifica sostanziale al sistema?	Critico	*Art. 43, Par. 4*
43	Il fornitore ha considerato le modifiche predeterminate apportate ai sistemi di IA ad alto rischio che proseguono il loro apprendimento come non costituenti una modifica sostanziale?	Critico	*Art. 43, Par. 4*

43	Il fornitore ha valutato se le modifiche apportate ai sistemi di IA ad alto rischio, che continuano ad apprendere dopo l'immissione sul mercato, rientrano tra quelle predeterminate al momento della valutazione iniziale della conformità e, quindi, non richiedono una nuova procedura di valutazione della conformità?	Critico	*Art. 43, Par. 4*

Dichiarazione di conformità UE - Comprendere e Applicare l'Articolo 47

# Articolo	Domanda	Livello di criticità	Richieste legislatore
47	Il fornitore ha compilato una dichiarazione di conformità UE per ogni sistema di IA ad alto rischio immesso sul mercato o messo in servizio, leggibile meccanicamente e firmata a mano o elettronicamente?	Critico	*Art. 47, Par. 1 Il fornitore deve redigere una dichiarazione di conformità UE per ogni sistema di IA ad alto rischio e mantenerla a disposizione delle autorità competenti per dieci anni. Il fornitore può ottenere il modello per la dichiarazione di conformità UE dall'allegato V del Regolamento sull'Intelligenza Artificiale dell'Unione Europea. L'allegato V specifica il contenuto minimo che deve essere incluso nella dichiarazione, come:* *1. il nome e il tipo del sistema di IA e qualsiasi ulteriore riferimento inequivocabile che ne consenta l'identificazione e la tracciabilità;* *2. il nome e l'indirizzo del fornitore o, ove applicabile, del suo rappresentante autorizzato;* *3. un'attestazione secondo cui la dichiarazione di conformità UE di cui all'articolo 47 è rilasciata sotto la responsabilità esclusiva del fornitore;* *4. un'attestazione secondo cui il sistema di IA è conforme al presente regolamento e, ove applicabile, a qualsiasi altra disposizione pertinente del diritto dell'Unione che preveda il rilascio di una dichiarazione di conformità UE di cui all'articolo 47;* *5. se un sistema di IA comporta il trattamento di dati personali, una dichiarazione attestante che tale sistema di IA è conforme ai regolamenti (UE) 2016/679 e (UE) 2018/1725 e alla direttiva (UE) 2016/680;* *6. i riferimenti alle pertinenti norme armonizzate utilizzate o a qualsiasi altra specifica comune in relazione alla quale è dichiarata la conformità;*

			7. ove applicabile, il nome e il numero di identificazione dell'organismo notificato, una descrizione della procedura di valutazione della conformità applicata e l'identificazione del certificato rilasciato; *8. il luogo e la data di rilascio della dichiarazione, il nome e la funzione della persona che firma la dichiarazione nonché un'indicazione della persona a nome o per conto della quale ha firmato, e la firma.*
47	Il fornitore ha tenuto a disposizione delle autorità nazionali competenti la dichiarazione di conformità UE per almeno dieci anni dalla data di immissione sul mercato o messa in servizio del sistema di IA ad alto rischio?	Importante	*Art 47 par 1 : La dichiarazione di conformità UE deve essere disponibile per un periodo di dieci anni.*
47	La dichiarazione di conformità UE attesta che il sistema di IA ad alto rischio soddisfa tutti i requisiti di cui alla sezione 2 del Regolamento?	Critico	*Art. 47, Par. 2 La dichiarazione deve certificare la conformità ai requisiti richiesti.*
47	Il fornitore ha tradotto la dichiarazione di conformità UE in una lingua facilmente comprensibile dalle autorità competenti degli Stati membri dove il sistema di IA è immesso sul mercato?	Critico	*Art. 47, Par. 2 La dichiarazione deve essere tradotta nella lingua appropriata per le autorità competenti.*
47	Se il sistema di IA ad alto rischio è soggetto anche ad altra normativa di armonizzazione dell'Unione, il fornitore ha redatto un'unica dichiarazione di conformità UE che include tutte le	Importante	*Art. 47, Par. 3 La dichiarazione di conformità UE deve coprire tutte le normative dell'Unione applicabili.*

	normative applicabili?		
47	Il fornitore ha aggiornato la dichiarazione di conformità UE quando necessario, per garantire la conformità continua ai requisiti di cui alla sezione 2 del Regolamento?	Critico	*Art. 47, Par. 4 Il fornitore deve mantenere la dichiarazione aggiornata per riflettere eventuali cambiamenti nei requisiti di conformità.*

Marcatura CE - Comprendere e Applicare l'Articolo 48

# Articolo	Domanda	Livello di criticità	Richieste legislatore
48	Il fornitore ha apposto la marcatura CE sul sistema di IA ad alto rischio in maniera visibile, leggibile e indelebile, ovvero sull'imballaggio o sui documenti di accompagnamento qualora non fosse possibile apporla direttamente sul sistema?	Critico	*La marcatura CE è apposta sul sistema di IA ad alto rischio in modo visibile, leggibile e indelebile. Qualora ciò sia impossibile o difficilmente realizzabile a causa della natura del sistema di IA ad alto rischio, il marchio è apposto sull'imballaggio o sui documenti di accompagnamento, a seconda dei casi.* (Art. 48, Par. 3)
48	Nel caso di sistemi di IA ad alto rischio forniti digitalmente, il fornitore ha utilizzato una marcatura CE digitale che è facilmente accessibile attraverso l'interfaccia del sistema o tramite un codice leggibile meccanicamente o altri mezzi elettronici facilmente accessibili?	Critico	Per i sistemi di IA ad alto rischio forniti digitalmente è utilizzata una marcatura CE digitale soltanto se è facilmente accessibile attraverso l'interfaccia da cui si accede a tale sistema o tramite un codice leggibile meccanicamente o altri mezzi elettronici facilmente accessibili (Art. 48, Par. 2)

48	Il fornitore ha apposto, ove applicabile, il numero di identificazione dell'organismo notificato responsabile della procedura di valutazione della conformità accanto alla marcatura CE, in conformità con le istruzioni ricevute dall'organismo notificato stesso?	Critico	Ove applicabile, la marcatura CE è seguita dal numero di identificazione dell'organismo notificato responsabile delle procedure di valutazione della conformità di cui all'articolo 43. Il numero di identificazione dell'organismo notificato è apposto dall'organismo stesso o, in base alle istruzioni di quest'ultimo, dal fornitore o dal rappresentante autorizzato del fornitore (Art. 48, Par. 4)
48	Il numero di identificazione dell'organismo notificato è stato inserito in tutti i materiali promozionali che dichiarano la conformità del sistema di IA ad alto rischio ai requisiti per la marcatura CE?	Importante	*Il numero d'identificazione è inoltre indicato in tutto il materiale promozionale in cui si afferma che il sistema di IA ad alto rischio soddisfa i requisiti per la marcatura CE.* (Art. 48, Par. 4)
48	Se i sistemi di IA ad alto rischio sono disciplinati da altre disposizioni del diritto dell'Unione che prevedono anch'esse l'apposizione della marcatura CE, il fornitore ha assicurato che la marcatura CE indica che il sistema soddisfa anche i requisiti delle altre normative in questione?	Critico	*Se i sistemi di IA ad alto rischio sono disciplinati da altre disposizioni del diritto dell'Unione che prevedono anch'esse l'apposizione della marcatura CE, quest'ultima indica che i sistemi di IA ad alto rischio soddisfano anche i requisiti delle altre normative in questione.* (Art. 48, Par. 5)

Registrazione - Comprendere e Applicare l'Articolo 49

# Articolo	Domanda	Livello di criticità	Richieste legislatore
49	Il fornitore o, ove applicabile, il rappresentante autorizzato ha registrato il sistema di IA ad alto rischio elencato nell'allegato III nella banca dati dell'UE prima di immetterlo sul mercato o metterlo in servizio?	Critico	*Prima di immettere sul mercato o mettere in servizio un sistema di IA ad alto rischio elencato nell'allegato III, il fornitore o, ove applicabile, il rappresentant*

			e autorizzato si registra e registra il suo sistema nella banca dati dell'UE di cui all'articolo 71. (Art. 49, Par. 1)
49	Il fornitore ha registrato un sistema di IA che ha concluso non essere ad alto rischio, secondo l'articolo 6, paragrafo 3, nella banca dati dell'UE prima della sua immissione sul mercato o messa in servizio?	Critico	*Prima di immettere sul mercato o mettere in servizio un sistema di IA che il fornitore ha concluso non essere ad alto rischio a norma dell'articolo 6, paragrafo 3, il fornitore o, ove applicabile, il rappresentante autorizzato si registra o registra tale sistema nella banca dati dell'UE di cui all'articolo 71."* (Art. 49, Par. 2)
49	I deployer che sono autorità pubbliche o persone che agiscono per conto di istituzioni pubbliche hanno registrato l'uso di un sistema di IA ad alto rischio elencato nell'allegato III, nella banca dati dell'UE, prima di metterlo in servizio o utilizzarlo?	Critico	*Prima di mettere in servizio o utilizzare un sistema di IA ad alto rischio elencato nell'allegato III, i deployer che sono autorità pubbliche, istituzioni, organi e organismi dell'Unione o persone che*

			agiscono per loro conto si registrano e ne registrano l'uso nella banca dati dell'UE di cui all'articolo 71." (Art. 49, Par. 3)
49	Il fornitore ha registrato i sistemi di IA ad alto rischio di cui all'allegato III, punti 1, 6 e 7, nei settori delle attività di contrasto, della migrazione, dell'asilo e della gestione del controllo delle frontiere, in una sezione sicura non pubblica della banca dati dell'UE?	Critico	*Per i sistemi di IA ad alto rischio di cui all'allegato III, punti 1, 6 e 7, nei settori delle attività di contrasto, della migrazione, dell'asilo e della gestione del controllo delle frontiere, la registrazione si trova in una sezione sicura non pubblica della banca dati dell'UE.* (Art. 49, Par. 4)
49	I sistemi di IA ad alto rischio di cui all'allegato III, punto 2, sono stati registrati a livello nazionale?	Critico	*I sistemi di IA ad alto rischio di cui all'allegato III, punto 2, sono registrati a livello nazionale.* (Art. 49, Par. 5)

Obblighi di trasparenza per i fornitori e i deployer di determinati sistemi di IA - Comprendere e Applicare l'Articolo 50

# Articolo	Domanda	Livello di criticità	Richieste legislatore
50	I fornitori garantiscono che le persone fisiche siano informate del fatto che stanno interagendo con un sistema di IA, a meno che non risulti evidente?	Critico	*Articolo 50, Par. 1*
50	I fornitori garantiscono che gli output dei sistemi di IA generanti contenuti siano marcati come generati o manipolati artificialmente?	Critico	*Articolo 50, Par. 2*
50	I deployer informano le persone fisiche sul funzionamento dei sistemi di riconoscimento delle emozioni o di categorizzazione biometrica?	Critico	*Articolo 50, Par. 3*
50	I deployer di sistemi che generano deep fake rendono noto che il contenuto è stato generato o manipolato artificialmente?	Critico	*Articolo 50, Par. 4*
50	Le informazioni sono fornite in modo chiaro e distinguibile al più tardi al momento della prima interazione o esposizione?	Critico	*Articolo 50, Par. 5 Le informazioni di cui ai paragrafi da 1 a 4 sono fornite alle persone fisiche interessate in maniera chiara e distinguibile al più tardi al momento della prima interazione o esposizione. Le informazioni devono essere conformi ai requisiti di accessibilità applicabili*

Classificazione dei modelli di IA per finalità generali come modelli di IA per finalità generali con rischio sistemico - Comprendere e Applicare l'Articolo 51

# Articolo	Domanda	Livello di criticità	Richieste legislatore
51	Il modello di IA per finalità generali presenta capacità di impatto elevato valutate sulla base di strumenti tecnici e metodologie adeguati, compresi indicatori e parametri di riferimento?	Critico	*Ai sensi dell'Art. 51, paragrafo 1, lettera a), un modello di IA per finalità generali è classificato come con rischio sistemico se presenta capacità di impatto elevato, valutate secondo parametri e strumenti tecnici.*
51	La quantità cumulativa di calcolo utilizzata per l'addestramento del modello di IA per finalità generali, misurata in operazioni in virgola mobile, supera 10^25?	Critico	*Ai sensi dell'Art. 51, paragrafo 2, un modello di IA per finalità generali è presunto avere capacità di impatto elevato se la quantità di calcolo cumulativa supera 10^25 operazioni.*

51	Avete verificato se la Commissione ha modificato le soglie relative ai parametri di impatto in base agli sviluppi tecnologici come miglioramenti algoritmici o efficienza hardware?	Critico	*Ai sensi dell'Art. 51, paragrafo 3, la Commission e può modificare i parametri di riferimento e soglie per il calcolo delle capacità di impatto in base a sviluppi tecnologici.*

Procedura - Comprendere e Applicare l'Articolo 52

# Articolo	Domanda	Livello di criticità	Richieste legislatore
52	Il fornitore ha informato la Commissione entro due settimane dal soddisfacimento della condizione di cui all'Articolo 51, paragrafo 1, lettera a?	Critico	*Art. 52, Par. 1: Il fornitore deve informare la Commissione senza ritardo e in ogni caso entro due settimane dal soddisfacimento della condizione.*
52	Il fornitore ha presentato argomentazioni sufficientemente fondate per dimostrare che il modello di IA non presenta rischi sistemici, sebbene soddisfi i requisiti di cui all'articolo 51, paragrafo 1?	Critico	*Art. 52, Par. 2: Il fornitore può presentare argomentazioni sufficientemente fondate per dimostrare che il modello non presenta rischi sistemici.*
52	La Commissione ha respinto le argomentazioni del fornitore e classificato il modello di IA come con rischio sistemico?	Critico	*Art. 52, Par. 3: La Commissione respinge le argomentazioni se non*

			sufficientemente fondate e classifica il modello come con rischio sistemico.
52	La Commissione ha designato un modello di IA come con rischio sistemico in seguito a una segnalazione qualificata del gruppo di esperti scientifici?	Critico	*Art. 52, Par. 4: La Commissione può designare un modello come con rischio sistemico in seguito a una segnalazione del gruppo di esperti scientifici.*
52	Il fornitore ha richiesto una nuova valutazione del modello di IA dopo sei mesi dalla decisione di designazione come modello con rischio sistemico?	Critico	*Art. 52, Par. 5: Il fornitore può richiedere una nuova valutazione del modello di IA dopo sei mesi dalla decisione di designazione.*

Obblighi dei fornitori di modelli di IA per finalità generali - Comprendere e Applicare l'Articolo 53

# Articolo	Domanda	Livello di criticità	Richieste legislatore
53	Il fornitore ha redatto e mantenuto aggiornata la documentazione tecnica del modello, compresi il processo di addestramento e prova?	Critico	*Il fornitore deve redigere e mantenere aggiornata la documentazione tecnica, come stabilito dall'Articolo 53, paragrafo 1, lettera a.*
53	Il fornitore ha messo a disposizione la documentazione per i fornitori di sistemi di IA che intendono integrare il modello?	Critico	*Il fornitore deve mettere a disposizione la documentazio*

			ne per i fornitori di sistemi di IA che integrano il modello, come stabilito dall'Articolo 53, paragrafo 1, lettera b.
53	Il fornitore ha attuato una politica di rispetto del diritto dell'Unione in materia di diritto d'autore?	Importante	*Il fornitore deve attuare una politica di rispetto del diritto d'autore, come stabilito dall'Articolo 53, paragrafo 1, lettera c.*
53	Il fornitore ha reso disponibile una sintesi dettagliata dei contenuti utilizzati per l'addestramento del modello?	Critico	*Il fornitore deve rendere disponibile una sintesi dettagliata dei contenuti di addestramento, come stabilito dall'Articolo 53, paragrafo 1, lettera d.*
53	Il fornitore ha collaborato con le autorità competenti nell'esercizio delle loro competenze?	Importante	*Il fornitore deve collaborare con le autorità competenti, come stabilito dall'Articolo 53, paragrafo 3.*

Rappresentanti autorizzati dei fornitori di modelli di IA per finalità generali - Comprendere e Applicare l'Articolo 54

# Articolo	Domanda	Livello di criticità	Richieste legislatore
54	Il fornitore, stabilito in un paese terzo, ha nominato un rappresentante autorizzato nell'Unione prima di immettere sul mercato il modello di IA?	Critico	*Art. 54, Par. 1: 'Prima di immettere sul mercato dell'Unione un modello di IA per finalità generali, i fornitori stabiliti in paesi terzi nominano, mediante mandato scritto, un rappresentante autorizzato stabilito nell'Unione.'*
54	Il rappresentante autorizzato ha eseguito i compiti specificati nel mandato del fornitore?	Critico	*Art. 54, Par. 2: 'Il fornitore consente al suo rappresentante autorizzato di eseguire i compiti specificati nel mandato ricevuto dal fornitore.'*
54	Il rappresentante autorizzato ha tenuto a disposizione delle autorità competenti la documentazione tecnica per 10 anni?	Importante	*Art. 54, Par. 3(b): 'Il rappresentante autorizzato tiene a disposizione una copia della documentazione tecnica per 10 anni dalla data in cui il modello di IA è stato immesso sul mercato.'*

54	Il rappresentante autorizzato ha fornito le informazioni richieste dall'ufficio per l'IA o dalle autorità competenti su richiesta motivata?	Importante	*Art. 54, Par. 3(c): 'Il rappresentante autorizzato fornisce, su richiesta motivata, tutte le informazioni necessarie per dimostrare la conformità agli obblighi.'*
54	Il rappresentante autorizzato ha cooperato con le autorità competenti per qualsiasi azione relativa al modello di IA?	Critico	*Art. 54, Par. 3(d): 'Il rappresentante autorizzato coopera con l'ufficio per l'IA e le autorità competenti.'*
54	Il rappresentante autorizzato ha cessato il mandato se il fornitore ha violato gli obblighi e ha informato l'ufficio per l'IA della cessazione?	Importante	*Art. 54, Par. 5: 'Il rappresentante autorizzato pone fine al mandato se ritiene che il fornitore agisca in contrasto con i propri obblighi.'*

Obblighi dei fornitori di modelli di IA per finalità generali con rischio sistemico - Comprendere e Applicare l'Articolo 55

# Articolo	Domanda	Livello di criticità	Richieste legislatore
55	Il fornitore ha effettuato una valutazione dei modelli secondo protocolli standardizzati e ha documentato il test contraddittorio per attenuare i rischi sistemici?	Critico	*Articolo 55(1a): Il fornitore deve effettuare una valutazione conforme a protocolli e strumenti standardizzati, inclusa la documentazione di un test contraddittorio (adversarial testing).*
55	Il fornitore ha valutato e attenuato i possibili rischi sistemici a livello dell'Unione derivanti dallo sviluppo o dall'uso del modello di IA?	Critico	*Articolo 55(1b): Il fornitore deve valutare e attenuare i rischi sistemici a livello dell'Unione, derivanti dallo sviluppo, dall'immissione sul mercato o dall'uso del modello.*
55	Il fornitore ha tracciato, documentato e riferito senza ritardi informazioni su incidenti gravi e misure correttive?	Importante	*Articolo 55(1c): Il fornitore deve tenere traccia e riferire senza ritardi le informazioni pertinenti su incidenti gravi e misure correttive all'Ufficio per l'IA e alle autorità nazionali.*

55	Il fornitore ha garantito un adeguato livello di cibersicurezza per il modello di IA e la sua infrastruttura fisica?	Importante	*Articolo 55(1d): Il fornitore deve garantire un livello adeguato di cibersicurezza per il modello di IA e la sua infrastruttura fisica.*

Conclusioni

Abbiamo attraversato insieme le complessità del Regolamento AI Act, esplorando passo dopo passo come assicurare che i sistemi di intelligenza artificiale siano conformi alle nuove normative europee. La compliance con l'AI Act non è solo un obbligo normativo, ma una grande opportunità per costruire un ambiente di innovazione tecnologica sicura, trasparente e centrata sull'essere umano. Seguendo le linee guida, è evidente come un approccio proattivo possa non solo evitare sanzioni, ma anche migliorare la qualità e la fiducia nei sistemi IA. La regolamentazione incoraggia la responsabilità e fornisce un quadro chiaro per il futuro, in cui le tecnologie avanzate come l'intelligenza artificiale possano prosperare senza compromettere i diritti fondamentali delle persone. Implementare misure come la valutazione dei rischi, la trasparenza e la supervisione umana non deve essere visto come un ostacolo, ma piuttosto come un modo per differenziarsi in un mercato sempre più competitivo. Sistemi di IA affidabili e sicuri non solo garantiranno la tua conformità normativa, ma rafforzeranno anche la fiducia dei tuoi clienti e partner.

In sintesi, l'AI Act rappresenta un passo fondamentale per il futuro dell'IA in Europa. Sfruttare questa normativa a proprio vantaggio significa adottare pratiche di compliance che, a lungo termine, rafforzeranno la reputazione e l'integrità del tuo business. La regolamentazione non è il punto di arrivo, ma l'inizio di un viaggio verso un'IA più etica, sicura e orientata al progresso umano.

Se hai seguito questa guida, sei sulla strada giusta per garantire che i tuoi sistemi IA siano in piena conformità con l'AI Act. Ricorda che la compliance non è un processo una tantum, ma richiede un monitoraggio costante e adattamenti continui in risposta a nuove sfide e sviluppi tecnologici.

Glossario

Termine dell'AI Act	Definizione secondo l'AI Act
Fornitore	Una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro ente che ha sviluppato un sistema di IA per immetterlo sul mercato o metterlo in servizio sotto il proprio nome o marchio, sia a pagamento che gratuitamente.
Deployer (Utilizzatore)	Una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro ente che utilizza un sistema di IA sotto la propria autorità.
Rappresentante autorizzato	Qualsiasi persona fisica o giuridica situata o stabilita nell'UE che ha ricevuto ed accettato un mandato scritto da un fornitore per eseguire i suoi obblighi per suo conto.
Importatore	Qualsiasi persona fisica o giuridica situata o stabilita nell'UE che immette sul mercato un sistema di IA che porta il nome o il marchio di una persona fisica o giuridica situata al di fuori dell'UE.
Distributore	Qualsiasi persona fisica o giuridica nella catena di approvvigionamento, che non è il fornitore o l'importatore, che rende disponibile un sistema di IA nel mercato dell'UE.
Produttore di prodotto	Un produttore di un sistema di IA che viene immesso sul mercato o un produttore che mette in servizio un sistema di IA insieme al proprio prodotto e sotto il proprio nome o marchio.
Operatore	Un termine generico che si riferisce a tutti i termini sopra menzionati (fornitore, deployer, rappresentante autorizzato, importatore, distributore o produttore di prodotto).