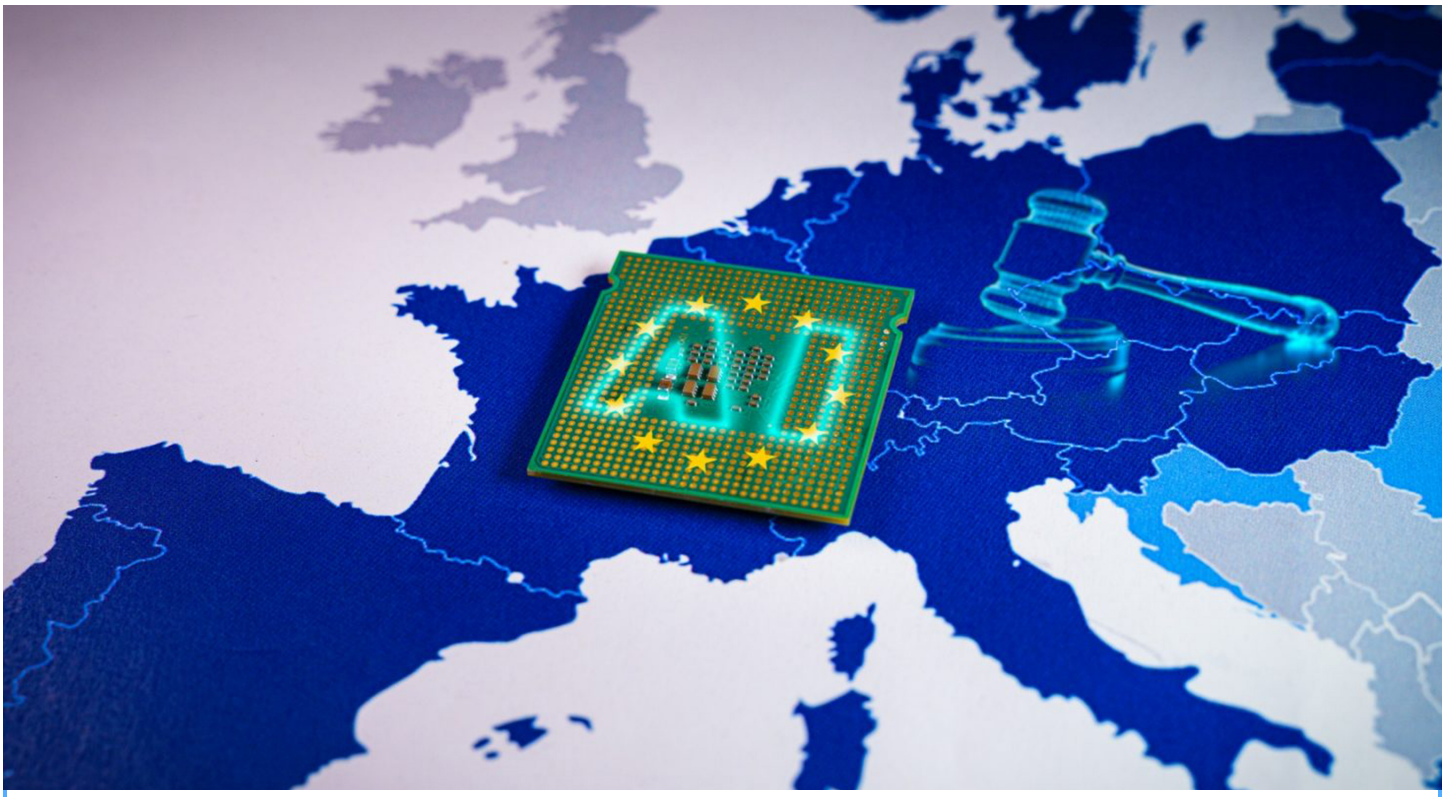
AI Act: il Regolamento europeo sull'intelligenza artificiale

di **Guido Scorza, Michela Massimi**
01/08/2025

INTELLIGENZA ARTIFICIALE REGOLAMENTO EUROPEO PRIMO BIENNIO



L'**AI Act**, **regolamento europeo** sull'**intelligenza artificiale**, promuove un'**innovazione responsabile e sicura**, stabilendo **quattro livelli di rischio** per disciplinare l'uso dei sistemi di IA. Le categorie vanno dai sistemi vietati (come quelli di manipolazione comportamentale) a quelli di rischio minimo, per i quali sono previsti requisiti di trasparenza.

Entrato in vigore ad agosto 2024, l'AI Act si applica in modo diretto nell'Unione Europea e prevede che fornitori e utenti rispettino norme specifiche in base al rischio del sistema. Gli obblighi includono gestione del rischio, trasparenza e monitoraggio post-mercato. Per i sistemi ad alto rischio, sono previste sanzioni significative per la non conformità, fino a 35 milioni di euro per le violazioni gravi.

Quattro livelli di rischio per promuovere la diffusione di un'intelligenza artificiale antropocentrica e affidabile, garantendo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali.

L'autore: *Guido Scorza è componente del Garante per la protezione dei dati personali. Si occupa di diritto delle nuove tecnologie, privacy e proprietà intellettuale da quasi trent'anni. Avvocato, giornalista pubblicista, docente in diverse università italiane e autore di numerose pubblicazioni, tra cui* "L'intelligenza artificiale, l'impatto sulle nostre vite, diritti e libertà"*, con Alessandro Longo, edito da Mondadori. È stato Consigliere giuridico del Ministro per l'innovazione e responsabile degli affari regolamentari nazionali ed europei del team per la trasformazione digitale della Presidenza del Consiglio dei Ministri.*

Michela Massimi collabora con Guido Scorza presso l'Autorità garante per la protezione dei dati personali.

Introduzione

Il 1° agosto 2024, venti giorni dopo la sua pubblicazione sulla Gazzetta Ufficiale dell'Unione europea, è entrato in vigore il Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024, che stabilisce **regole armonizzate sull'intelligenza artificiale** (noto anche come Regolamento sull'intelligenza artificiale o **AI Act**).

Il Regolamento diventerà direttamente applicabile nei Paesi dell'Unione in maniera progressiva tra il 2 agosto 2024 e il 2 agosto 2027. Ciò al fine di consentire ai Paesi membri e ai mercati di prepararsi al suo adempimento.

L'iter che ha portato all'approvazione dell'AI Act è durato poco più di tre anni, un intervallo di tempo oggettivamente breve in considerazione della complessità della materia e di quella dei processi di regolamentazione europea. Ora l'Unione europea e i suoi Stati membri sono i primi al mondo ad avere una legge organica in materia di intelligenza artificiale, le cui disposizioni si applicheranno a tutti i soggetti, pubblici e privati, all'interno e all'esterno dell'Unione, che producono, distribuiscono e utilizzano in maniera professionale sistemi di intelligenza artificiale destinati al mercato europeo o il cui uso riguardi persone che vivono nell'Unione.

Essere stati i primi al mondo, tuttavia, non è sufficiente. La vera gara, infatti, non è tra gli Stati, ma tra gli Stati, il mercato e l'industria.

La scommessa nel governo di un fenomeno globale e pervasivo come quello dell'intelligenza artificiale, infatti, è fare in modo che il suo impatto sulla società sia regolato dagli Stati e non dall'industria attraverso la semplice diffusione di prodotti e servizi capaci di plasmare le nostre vite più e prima di quanto facciano le leggi.

Gli **obiettivi principali dell'AI Act** sono:

- promuovere l'innovazione responsabile, incoraggiando lo sviluppo di tecnologie AI all'interno di un ambiente normativo sicuro e controllato;
- proteggere i cittadini, garantendo che i diritti fondamentali, come la privacy, la sicurezza e la non discriminazione, siano salvaguardati;
- favorire la fiducia, aumentando la trasparenza e la comprensione dell'AI per far sì che i cittadini possano fidarsi delle tecnologie con cui interagiscono.

Per raggiungere questi obiettivi il legislatore europeo ha utilizzato un **approccio basato sul rischio**, imponendo ai protagonisti dell'industria e del mercato di riferimento obblighi crescenti, in maniera direttamente proporzionale all'aumentare della rischiosità dei prodotti e servizi sviluppati, commercializzati e/o utilizzati professionalmente.

A tal fine, le tipologie di prodotti e servizi basati sull'AI sono state classificate in 4 livelli:
sistemi di AI a rischio inaccettabile: sono quelli che rappresentano un rischio così elevato per i diritti fondamentali che vengono vietati completamente. Un esempio è l'uso di AI per manipolare il comportamento umano in modi che mettano a rischio la sicurezza o la salute;
sistemi di AI ad alto rischio: includono tecnologie che possono avere un impatto significativo su sicurezza e diritti delle persone. Questi sistemi devono rispettare requisiti rigorosi, come la trasparenza, la supervisione umana e la qualità dei dati. Esempi includono i sistemi di riconoscimento facciale o le AI utilizzate in ambito medico e lavorativo;
sistemi di AI a rischio limitato: richiedono solo il rispetto di alcune norme sulla trasparenza, come informare gli utenti che vi interagiscono. Un esempio è una chatbot che risponde a domande di assistenza clienti;
sistemi di AI a rischio minimo: in questa categoria rientrano le applicazioni di AI più comuni e diffuse, come filtri antispam o raccomandazioni di contenuti online. Questi sistemi non necessitano di particolari regolamentazioni, se non il rispetto delle norme generali di sicurezza e privacy.
Nei paragrafi successivi si illustreranno in maniera più puntuale le caratteristiche della nuova disciplina.

L’AI Act nel sistema delle fonti

Il legislatore europeo ha scelto di disciplinare la materia con un **regolamento**, ossia un atto che ha portata generale, è obbligatorio in tutti i suoi elementi e direttamente applicabile senza necessità di recepimento nel diritto nazionale e che deve essere pienamente rispettato dai destinatari (privati, Stati membri, istituzioni dell’Unione).

Lo scopo è quello di garantire l’**applicazione uniforme della nuova normativa in tutti gli Stati membri**, escludendo così il rischio di asimmetrie regolamentari per effetto delle quali taluni beni o servizi, la loro produzione, la loro distribuzione o il loro utilizzo potrebbero essere disciplinati in modo diverso da Paese a Paese.

Per questa ragione è stato preferito il regolamento alla direttiva, che invece avrebbe vincolato gli Stati membri per quanto riguarda il risultato da raggiungere, lasciando alla competenza degli organi nazionali la scelta di forma e mezzi, e la cui applicazione nel diritto interno avrebbe richiesto l’adozione da parte dello Stato di un atto di recepimento, non essendo le direttive, in linea di principio, direttamente applicabili.

Le scadenze previste per l’attuazione

Come si è anticipato, le previsioni contenute nel Regolamento non diverranno tutte applicabili nello stesso momento ma gradatamente, sulla base dell’urgenza di disciplinare taluni aspetti prima di altri e, soprattutto, di garantire agli Stati membri e ai mercati il tempo necessario per adempiere alle nuove regole.

LA TABELLA DI MARCIA	
20 giorni dopo la pubblicazione nella Gazzetta Ufficiale	Entrata in vigore della legge
2 febbraio 2025	Divieto sui sistemi di IA con rischio inaccettabile (ad esempio, identificazione biometrica)
2 maggio 2025	Applicazione dei codici di condotta
2 agosto 2025	Applicazione delle regole di governance e degli obblighi per l'AI di scopo generale (ad esempio, ChatGPT) e delle disposizioni relative alle sanzioni
2 agosto 2026	Applicazione di tutte le norme del regolamento
2 agosto 2027	Applicazione degli obblighi per i sistemi ad alto rischio

Il *Considerando 174* del regolamento prevede poi che, in considerazione dei «rapidi sviluppi tecnologici e [del]le competenze tecniche necessarie per applicare efficacemente il presente regolamento, la Commissione dovrebbe valutare e riesaminare il presente regolamento entro il 2 agosto 2029 e successivamente ogni quattro anni e riferire al Parlamento europeo e al Consiglio».

E aggiunge che «entro il 2 agosto 2028 e successivamente ogni quattro anni, la Commissione dovrebbe valutare e riferire al Parlamento europeo e al Consiglio sulla necessità di modificare l'elenco delle voci relative alle aree ad alto rischio nell'allegato del presente regolamento, i sistemi di AI nell'ambito degli obblighi di trasparenza, l'efficacia del sistema di supervisione e governance e i progressi nello sviluppo di risultati di normazione sullo sviluppo efficiente dal punto di vista energetico di modelli di AI di uso generale, compresa la necessità di ulteriori misure o azioni».

Entro la stessa data «e successivamente ogni tre anni, la Commissione dovrebbe valutare l'impatto e l'efficacia dei codici di condotta volontari per promuovere l'applicazione dei requisiti previsti per i sistemi di IA ad alto rischio nel caso di sistemi di AI diversi dai sistemi di IA ad alto rischio ed eventualmente altri requisiti aggiuntivi per tali sistemi di AI».

Struttura e contenuto dell'AI Act

La struttura dell'AI Act, come si è anticipato, è caratterizzata da diversi livelli di rischio per i sistemi di intelligenza artificiale, a seconda del loro potenziale impatto sui cittadini, in funzione dei quali sono diversamente modulati misure e adempimenti da adottare.

In particolare, vengono individuati i **quattro livelli di rischio** (minimo, limitato, alto e inaccettabile): al crescere del rischio aumentano anche le responsabilità e i limiti nello sviluppo e nell'uso dei sistemi di intelligenza artificiale, sino ad arrivare ai modelli troppo pericolosi e, quindi, semplicemente vietati.

L'AI Act contiene un ampio quadro di divieti, di obblighi e di requisiti relativi ai sistemi di intelligenza artificiale, nonché un sistema sanzionatorio.

Come accennato, lo **scopo principale dell'AI Act** «è migliorare il funzionamento del mercato interno istituendo un quadro giuridico uniforme in particolare per quanto riguarda lo sviluppo, l'immissione sul mercato, la messa in servizio e l'uso di sistemi di intelligenza artificiale nell'Unione, in conformità dei valori dell'Unione, promuovere la diffusione di un'intelligenza artificiale [...] antropocentrica e affidabile, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea [...], compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, proteggere contro gli effetti nocivi dei sistemi di AI nell'Unione, nonché promuovere l'innovazione» (così il Considerando 1). Inoltre, il Regolamento «garantisce la libera circolazione transfrontaliera di beni e servizi basati sull'AI, impedendo così agli Stati membri di imporre restrizioni allo sviluppo, alla commercializzazione e all'uso di sistemi di AI, salvo espressa autorizzazione del regolamento».

La normativa si articola in **tredici Capi e 113 articoli**.

Il primo Capo è intitolato *Disposizioni generali* e contiene le **definizioni**, prima fra tutte quella di **sistema di IA**, ossia «un sistema automatizzato progettato per operare con livelli di autonomia variabili, che può mostrare 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».

Sotto il profilo soggettivo, il Regolamento identifica *in primis* il "fornitore" e il "deployer".

Il **fornitore** è da intendersi come la persona fisica o giuridica, Autorità pubblica, Agenzia o altro organismo che sviluppa o fa sviluppare un sistema di intelligenza artificiale sotto la propria direzione e controllo, e lo immette sul mercato nell'Unione europea sia per commercializzarlo sia per metterlo in funzione per uso proprio/interno.

Il **deployer** è definito come la persona fisica o giuridica, Autorità pubblica, Agenzia o altro Organismo che nell'ambito della propria attività professionale (sono escluse le persone fisiche che utilizzano sistemi di IA per attività puramente personali) utilizza un sistema di AI sotto la propria autorità.

Dalla qualifica soggettiva dipendono gli **adempimenti** previsti dal Regolamento.

Il fornitore ha l'onere di predisporre un sistema di gestione dei rischi; adottare misure di governance dei dati; preparare - e conservare - un'articolata documentazione tecnica per sottoporre il sistema di IA a una procedura di valutazione della conformità (marcatura CE); fornire istruzioni accurate ai deployer; impostare in fase di progettazione un adeguato livello di resilienza rispetto a malfunzionamenti o attacchi cyber.

Viceversa, il deployer deve rigorosamente attenersi alle istruzioni d'uso ricevute dal fornitore, assicurare la sorveglianza umana sul sistema di AI e affidarla a persone competenti e formate; monitorare il funzionamento del sistema e in caso di incidenti, informare immediatamente il fornitore e l'Autorità di vigilanza; in caso di decisioni sulle persone deve informare gli interessati sul ruolo dell'AI. Infine, se la qualifica di deployer è in capo a Pubblica Amministrazione, banche e assicurazioni, nel caso di sistemi di credit scoring o risk assessment e pricing assicurativo, è necessario redigere una valutazione dell'impatto sui diritti fondamentali.

Oltre che a fornitori e deployer, le nuove regole dell'AI Act si applicano anche agli importatori e ai distributori di sistemi di IA; ai fabbricanti di prodotti che immettono sul mercato o mettono in servizio un sistema di AI insieme al loro prodotto e con il loro nome o marchio; ai rappresentanti autorizzati di fornitori, non stabiliti nell'Unione; alle persone interessate che si trovano nell'Unione.

Il Capo II (**Pratiche di intelligenza artificiale vietate**) contiene un solo articolo (art. 5), che elenca una serie di sistemi di AI vietati in quanto connotati da un livello di rischio inaccettabile per la sicurezza delle persone.

Si tratta dei sistemi che utilizzano tecniche subliminali in grado di manipolare le persone, inducendole a prendere una decisione che non avrebbero mai preso, compresi quelli che sfruttano a tal fine vulnerabilità dovute all'età, alla disabilità o a una specifica situazione sociale o economica; i sistemi di punteggio sociale in grado di classificare le persone in base al loro comportamento sociale o alle loro caratteristiche personali; i sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico; i sistemi di categorizzazione biometrica basati su caratteristiche sensibili quali genere, razza, etnia, cittadinanza, religione, orientamento politico; i sistemi di polizia predittiva basati su profilazione, ubicazione o comportamenti criminali passati; i sistemi di riconoscimento delle emozioni utilizzati dalle forze dell'ordine, nella gestione delle frontiere, nel luogo di lavoro e negli istituti d'istruzione; i sistemi che creano o ampliano le banche dati di riconoscimento facciale mediante scraping non mirato di immagini facciali da internet o da filmati di telecamere a circuito chiuso.

Con specifico riguardo ai sistemi di identificazione biometrica "in tempo reale" in spazi accessibili al pubblico, l'art. 5 ne consente l'uso esclusivamente se strettamente necessario a fini di attività di contrasto in alcune specifiche ipotesi (ad esempio, ricerca di persone scomparse; prevenzione di attacco terroristico; identificazione di sospettati di particolari reati) e comunque "solo per confermare l'identità della persona specificamente interessata" e previa autorizzazione rilasciata da un'autorità giudiziaria o da un'autorità amministrativa indipendente dello Stato membro in cui deve avvenire l'uso.

È importante ricordare che anche nei casi in cui l'uso dei suindicati sistemi è ammesso «Nessuna decisione che produca effetti giuridici negativi su una persona può essere presa unicamente sulla base dell'output del sistema di identificazione biometrica remota "in tempo reale"» (così l'art. 5, par. 3).

Subito dopo i sistemi vietati, l'AI Act disciplina al Capo III quelli **ad alto rischio**, definendo le condizioni in presenza delle quali i sistemi di AI debbano ricevere tale qualifica e individuandone un primo gruppo, che comprende quelli destinati a essere utilizzati come componenti di sicurezza di prodotti (macchine, giocattoli, dispositivi medici, veicoli a motore e così via) soggetti a valutazione di conformità ex ante da parte di terzi, secondo quanto previsto dall'Allegato I del Regolamento.

Il secondo gruppo dei sistemi di AI ad alto rischio viene individuato nell'Allegato III e comprende specifici settori: la biometria, nella misura in cui il diritto dell'UE o nazionale ne permette l'uso; le infrastrutture critiche; i sistemi di istruzione e formazione professionale; i sistemi di occupazione, gestione dei lavoratori e accesso al lavoro autonomo; i sistemi di accesso a servizi privati essenziali e a prestazioni e servizi pubblici essenziali; le attività di contrasto, nella misura in cui il diritto dell'UE o nazionale ne permette l'uso; i sistemi di migrazione, asilo e gestione del controllo delle frontiere; i sistemi di amministrazione della giustizia e processi democratici.

In ogni caso, un sistema di AI di cui all'Allegato III non può essere considerato ad alto rischio se non è capace di "influenzare materialmente il risultato del processo decisionale" o se non presenta altrimenti un rischio significativo di danno per la salute, la sicurezza o i diritti fondamentali delle persone fisiche. Per converso, un sistema di AI di cui all'Allegato III è sempre considerato ad alto rischio qualora effettui la **profilazione di persone fisiche**.

Per i sistemi ad alto rischio il Regolamento detta un'articolata disciplina concernente, tra l'altro, la conformità ai requisiti, il sistema di gestione dei rischi, la governance dei dati utilizzati per l'addestramento degli algoritmi, gli specifici obblighi dei fornitori e dei deployer, la cooperazione con le autorità competenti, la valutazione d'impatto sui diritti fondamentali, la procedura di notifica.

Specifici **obblighi di trasparenza** sono previsti dal Capo IV per i fornitori e i deployer di determinati sistemi di AI, come i sistemi che interagiscono con le persone fisiche, i sistemi per finalità generali che generano contenuti audio, immagine, video o testuali sintetici (ad esempio, ChatGPT), i sistemi di riconoscimento delle emozioni e quelli di categorizzazione biometrica. Per tali sistemi sono previsti obblighi informativi chiari finalizzati a rendere le persone consapevoli della natura dei rischi. I fornitori di sistemi che generano contenuti audio, immagine, video o testuali sintetici garantiscono inoltre che gli output del sistema siano marcati in un formato leggibile meccanicamente e rilevabili come generati o manipolati artificialmente.

Il Capo V disciplina i **modelli di IA per finalità generali**, prevedendo che gli stessi siano classificati come modelli "con rischio sistemico" in presenza di determinate condizioni (ad esempio, capacità di impatto elevato) e individuando per i loro fornitori una serie di adempimenti, anche di carattere informativo e documentale.

Il Capo VI, intitolato **Misure a sostegno dell'innovazione**, contiene la disciplina degli spazi di sperimentazione normativa (le c.d. **sandboxes**), stabilendo che tali spazi garantiscano un ambiente controllato che promuove l'innovazione e facilita lo sviluppo, l'addestramento, la sperimentazione e la convalida di sistemi di AI innovativi per un periodo di tempo limitato, prima della loro immissione sul mercato o della loro messa in servizio conformemente a un piano specifico dello spazio di sperimentazione concordato tra i fornitori o i potenziali fornitori e l'autorità competente.

Vengono inoltre disciplinate le prove dei sistemi ad alto rischio in condizioni reali al di fuori dei sandboxes e previste misure volte ad agevolare particolari fornitori e deployer, quali le PMI, comprese le start-up, ad esempio concedendo loro un accesso prioritario agli spazi di sperimentazione normativa per l'AI nella misura in cui soddisfino le condizioni di ammissibilità e i criteri di selezione pure previsti.

La **governance**, ovvero il sistema attraverso il quale si dovrà dare attuazione alle regole contenute nell'AI Act, è disciplinata dal Capo VII, ove è stabilito che l'ufficio per l'AI della Commissione (**AI Office**) sarà l'organo per l'implementazione dell'AI Act al livello dell'Unione. Sono previsti tre organi consultivi con funzioni di supporto nell'implementazione delle norme: il **Comitato europeo per l'intelligenza artificiale**, un gruppo di esperti scientifici indipendenti selezionati dalla Commissione e un **forum consultivo** che comprende diversi stakeholders selezionati tra società civile, mondo accademico, start-up e PMI. Gli Stati membri, a loro volta, devono individuare almeno un'**Autorità di notifica** e un'**Autorità di vigilanza del mercato** che supervisionino l'applicazione delle norme del Regolamento.

Nel Capo VIII viene disciplinata la **banca dati dell'UE per i sistemi di IA ad alto rischio**, che deve essere istituita e mantenuta dalla Commissione in collaborazione con gli Stati membri e nella quale i fornitori devono inserire i dati elencati nell'Allegato VIII del Regolamento. Tra questi ci saranno informazioni quali la denominazione commerciale del sistema di IA, il nome, l'indirizzo e i dati di contatto del fornitore, una descrizione di base concisa delle informazioni utilizzate dal sistema (dati, input) e della sua logica operativa, lo status del sistema di AI (sul mercato, o in servizio, non più immesso sul mercato/in servizio, richiamato).

È previsto, inoltre, che salvo alcune eccezioni (ad esempio per i sistemi in uso nei settori delle attività di contrasto, della migrazione, dell'asilo e della gestione del controllo delle frontiere), le informazioni contenute nella banca dati siano accessibili e disponibili al pubblico in modo facilmente fruibile.

Il Regolamento prevede al Capo IX che i fornitori debbano istituire e documentare un **sistema di monitoraggio** successivo all'immissione sul mercato, che sia proporzionato alla natura delle tecnologie di AI utilizzate e ai rischi. Tale sistema di monitoraggio, attraverso la raccolta, la documentazione e l'analisi delle prestazioni dei sistemi di AI ad alto rischio per tutta la durata del loro ciclo di vita, consentirà al fornitore di valutarne la costante conformità ai requisiti previsti, anche al fine di adempiere all'obbligo di comunicare eventuali incidenti gravi occorsi ai propri sistemi previsto dall'art. 73.

Tale disposizione prevede altresì che la segnalazione sia effettuata dal fornitore immediatamente dopo che lo stesso abbia stabilito un nesso causale tra il sistema di AI e l'incidente grave o la ragionevole probabilità di tale nesso e, in ogni caso, non oltre 15 giorni dopo che ne sia venuto a conoscenza.

Sempre nell'ambito del monitoraggio, il Regolamento riconosce a chiunque (persona fisica o giuridica) abbia motivo di ritenere che vi sia stata una violazione delle proprie disposizioni il diritto di presentare un **reclamo alla pertinente autorità di vigilanzadel mercato**, fatti salvi altri ricorsi amministrativi o giurisdizionali (art. 85).

Il Regolamento contiene al Capo X previsioni volte a incoraggiare le imprese a elaborare **codici di condotta e meccanismi di governance** intesi a promuovere l'applicazione volontaria ai sistemi di AI, diversi da quelli ad alto rischio, di alcuni o di tutti i requisiti previsti per i sistemi ad alto rischio dal Capo III, mentre il Capo XI prevede le condizioni e i termini temporali ai quali è conferito alla Commissione il potere di adottare atti delegati ai sensi del Regolamento.

Il Capo XII riguarda il **regime delle sanzioni** e delle altre misure di esecuzione che gli Stati membri devono applicare in caso di violazione del Regolamento. Esso prevede che le stesse possano includere avvertimenti e misure non pecuniarie e debbano essere effettive, proporzionate e dissuasive, dovendo tener conto anche degli interessi delle PMI, comprese le start-up, e della loro sostenibilità economica.

I limiti edittali previsti dall'AI Act sono molto elevati, in particolare con riguardo alla non conformità al divieto delle pratiche di AI di cui all'art. 5, soggetta a sanzioni amministrative pecuniarie fino a 35.000.000 di euro o, se l'autore del reato è un'impresa, fino al 7% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

Il limite è, invece, di 15.000.000 di euro (fino al 3% del fatturato mondiale totale annuo dell'esercizio precedente se superiore, per le imprese) per i casi di non conformità alle diverse, specifiche disposizioni richiamate nell'art. 99, par. 4, mentre la fornitura di informazioni inesatte, incomplete o fuorvianti agli organismi notificati o alle autorità nazionali competenti per dare seguito a una richiesta è soggetta a sanzioni amministrative pecuniarie fino a 7.500.000 euro (fino all'1% del fatturato mondiale totale annuo dell'esercizio precedente se superiore, per le imprese).

Chiude il Regolamento il Capo XIII, che comprende le previsioni relative alle diverse **scadenze**, delle quali si è già riferito.