Regolamento sull'Intelligenza Artificiale (AI Act) - SINTESI

1. Oggetto e Scopo del Regolamento (Articolo 1)

Il regolamento ha come obiettivo primario il **miglioramento del funzionamento del mercato interno** stabilendo un **quadro giuridico uniforme** per lo sviluppo, l'immissione sul mercato, la messa in servizio e l'uso dei sistemi di intelligenza artificiale (IA) nell'Unione Europea. Si propone di promuovere un'IA **antropocentrica e affidabile**, garantendo al contempo un **elevato livello di protezione della salute, della sicurezza e dei diritti fondamentali** sanciti dalla Carta dei diritti fondamentali dell'Unione europea, inclusi la democrazia, lo Stato di diritto e la protezione dell'ambiente. Un altro scopo è **proteggere contro gli effetti nocivi dei sistemi di IA nell'Unione** e **promuovere l'innovazione e l'occupazione**, rendendo l'Unione un leader nell'adozione di un'IA affidabile.

2. Ambito di Applicazione (Articolo 2)

Il regolamento si applica a una vasta gamma di attori e situazioni, tra cui:

- Fornitori che immettono sul mercato o mettono in servizio sistemi di IA o modelli di IA per finalità generali nell'Unione.
- Deployer (utilizzatori) di sistemi di IA stabiliti nell'Unione.
- Fornitori e deployer stabiliti in paesi terzi, nella misura in cui l'output dei loro sistemi di IA è destinato a essere utilizzato nell'Unione, al fine di prevenire elusioni e garantire protezione efficace.
- Importatori, distributori, rappresentanti autorizzati e le persone interessate che si trovano nell'Unione.

Esclusioni chiave:

- Settori al di fuori dell'ambito del diritto dell'Unione e competenze degli Stati membri in materia di **sicurezza nazionale** (indipendentemente dal tipo di entità).
- Sistemi di IA utilizzati **esclusivamente per scopi militari e di difesa**.
- Autorità pubbliche di paesi terzi o organizzazioni internazionali che utilizzano sistemi di IA nell'ambito della **cooperazione internazionale di forze dell'ordine e giudiziarie**, a condizione che forniscano garanzie adeguate per i diritti e le libertà fondamentali.
- Sistemi o modelli di IA specificamente sviluppati e messi in servizio **al solo scopo di ricerca e sviluppo scientifici**.
- Attività di ricerca, prova o sviluppo di sistemi o modelli di IA prima della loro immissione sul mercato o messa in servizio.
- Sistemi di IA rilasciati con **licenza libera e open source**, a meno che non siano immessi sul mercato o messi in servizio come sistemi di IA ad alto rischio o rientrino negli articoli 5 (pratiche vietate) o 50 (obblighi di trasparenza).
- Il regolamento non pregiudica l'applicazione delle normative sulla protezione dei dati personali (GDPR, Direttiva 2016/680, Direttiva 2002/58/CE).

3. Definizione di "Sistema di IA" (Articolo 3, Punto 1)

Il regolamento fornisce una definizione chiara e flessibile per "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." (Articolo 3, Punto 1)

Viene sottolineata la **capacità inferenziale** che distingue l'IA dai software tradizionali, consentendo l'apprendimento, il ragionamento o la modellizzazione da input o dati.

4. Approccio Basato sul Rischio (Considerando 26)

Il regolamento adotta un **approccio basato sul rischio** per regolare l'IA, adattando il tipo e il contenuto delle regole all'intensità e alla portata dei rischi. Questo include:

- Divieto di determinate pratiche di IA "inaccettabili".
- Requisiti per i sistemi di IA "ad alto rischio" e obblighi per i relativi operatori.
- Obblighi di trasparenza per determinati sistemi di IA.

5. Pratiche di IA Vietate (Articolo 5)

Sono vietate le pratiche di IA che sono considerate particolarmente dannose e abusive, in quanto contrarie ai valori dell'Unione e ai diritti fondamentali. Queste includono:

- **Sistemi di IA che utilizzano tecniche subliminali, manipolative o ingannevoli** per distorcere materialmente il comportamento di una persona, causando danni significativi. (Articolo 5, Paragrafo 1, Lettera a)
- **Sfruttamento di vulnerabilità** di persone o gruppi (età, disabilità, situazione sociale/economica) per distorcere materialmente il loro comportamento e causare danni significativi. (Articolo 5, Paragrafo 1, Lettera b)
- **Sistemi di "punteggio sociale"** che classificano persone o gruppi in base al comportamento sociale o tratti personali, risultando in trattamenti pregiudizievole o sproporzionati. (Articolo 5, Paragrafo 1, Lettera c)
- **Valutazione del rischio di criminalità** basata unicamente sulla profilazione o tratti della personalità. Non si applica a sistemi a supporto di valutazioni umane basate su fatti oggettivi e verificabili. (Articolo 5, Paragrafo 1, Lettera d)
- **Creazione o ampliamento di banche dati di riconoscimento facciale mediante scraping non mirato** da internet o filmati di telecamere a circuito chiuso. (Articolo 5, Paragrafo 1, Lettera e)
- **Sistemi di riconoscimento delle emozioni in ambito lavorativo o educativo**, salvo per scopi medici o di sicurezza sul lavoro. (Articolo 5, Paragrafo 1, Lettera f)
- **Sistemi di categorizzazione biometrica basati su dati sensibili** (opinioni politiche, etnia, orientamento sessuale, ecc.). Questo divieto non si applica all'etichettatura o filtraggio di set di dati biometrici acquisiti legalmente per scopi di forze dell'ordine. (Articolo 5, Paragrafo 1, Lettera g)
- **Uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico da parte delle forze dell'ordine**, salvo in situazioni eccezionali e rigorosamente definite, previa autorizzazione giudiziaria o amministrativa indipendente. Le eccezioni includono la ricerca di vittime (rapimenti, tratta), prevenzione di minacce gravi e imminenti (terrorismo, vita/incolumità fisica), e localizzazione/identificazione di sospettati di reati gravi (punibili con almeno quattro anni di reclusione, come elencati nell'Allegato II). (Articolo 5, Paragrafo 1, Lettera h)

L'uso di sistemi di identificazione biometrica remota "a posteriori" (non in tempo reale) è consentito con tutele, ma non deve essere usato per sorveglianza indiscriminata. (Considerando 95)

6. Sistemi di IA ad Alto Rischio (Articolo 6 e Allegato III)

I sistemi di IA sono classificati come ad alto rischio se:

- Sono componenti di sicurezza di prodotti soggetti a una valutazione di conformità da parte di terzi ai sensi della normativa di armonizzazione dell'Unione (Allegato I, Sezione A). (Articolo 6, Paragrafo 1)
- Rientrano in categorie specifiche elencate nell'Allegato III. (Articolo 6, Paragrafo 2)

Casi di IA ad alto rischio elencati nell'Allegato III:

- **Identificazione biometrica e categorizzazione di persone fisiche:** Sistemi di identificazione biometrica remota (esclusa la verifica biometrica).
 - Sistemi di categorizzazione biometrica basati su attributi sensibili.
 - Sistemi di riconoscimento delle emozioni.
1. **Infrastrutture critiche:** Sistemi di IA utilizzati come componenti di sicurezza nella gestione di infrastrutture digitali critiche, traffico stradale, o fornitura di acqua, gas, riscaldamento o elettricità.
 2. **Istruzione e formazione professionale:** Sistemi di IA per determinare l'accesso, l'ammissione, l'assegnazione a istituti di istruzione/formazione, o per valutare gli studenti (es. esami, rilevamento frodi).
 3. **Occupazione, gestione dei lavoratori e accesso al lavoro autonomo:** Sistemi di IA per assunzione, selezione, decisioni su condizioni di lavoro, assegnazione di compiti basati su comportamento/tratti personali, monitoraggio o valutazione delle prestazioni/comportamento dei lavoratori.
- **Accesso e fruizione di servizi privati essenziali e servizi pubblici essenziali:** Sistemi di IA per valutare l'ammissibilità a prestazioni e servizi pubblici essenziali (sanità, sicurezza sociale, servizi sociali).
 - Sistemi di IA per valutare il merito o l'affidabilità creditizia di persone fisiche (esclusi quelli per individuare frodi finanziarie o per requisiti prudenziali di enti finanziari).
 - Sistemi di IA per la valutazione dei rischi e la determinazione dei prezzi in assicurazioni sulla vita e sanitarie.
 - Sistemi di IA per valutare e classificare chiamate di emergenza o per l'invio/prioritizzazione di servizi di emergenza e selezione dei pazienti in assistenza sanitaria di emergenza.
1. **Attività di contrasto:** (se consentito dal diritto UE/nazionale)
 - Sistemi di IA per determinare il rischio che una persona diventi vittima di reati.
 - Poligrafi e strumenti analoghi.
 - Sistemi di IA per valutare l'affidabilità delle prove in indagini/procedimenti penali.
 - Sistemi di IA per determinare il rischio di criminalità o recidiva (non solo basati su profilazione, ma anche tratti della personalità o comportamento criminale pregresso).
 - Sistemi di IA per la profilazione di persone fisiche in indagini/procedimenti penali.
 1. **Migrazione, asilo e gestione del controllo delle frontiere:** (se consentito dal diritto UE/nazionale)
 - Sistemi di IA per valutare il rischio di ingresso non autorizzato.
 - Sistemi di IA per verificare l'autenticità dei documenti di viaggio.
 - Sistemi di IA per valutare l'ammissibilità all'asilo o ai visti.
 - Sistemi di IA per assistere le autorità nel controllo delle frontiere, nell'immigrazione o nell'asilo (escluse verifiche di identità standard).
 - **Amministrazione della giustizia e processi democratici:** Sistemi di IA per assistere le autorità giudiziarie o amministrative nella ricerca e interpretazione dei fatti e del diritto e nell'applicazione della legge a casi specifici.
 - Sistemi di IA per influenzare l'esito di elezioni o referendum o il comportamento di voto.

Deroga alla classificazione ad alto rischio: Un sistema di IA dell'Allegato III non è considerato ad alto rischio se non presenta un rischio significativo di danno per la salute, la sicurezza o i diritti fondamentali, ad esempio se svolge un compito procedurale limitato, migliora un'attività umana già completata, rileva schemi decisionali senza influenzare la valutazione umana, o svolge un compito preparatorio. Tuttavia, se comporta la profilazione di persone fisiche, è **sempre** considerato ad alto rischio. (Articolo 6, Paragrafo 3)

7. Requisiti per i Sistemi di IA ad Alto Rischio (Sezione 2, Capo III)

I fornitori di sistemi di IA ad alto rischio devono garantire la conformità a una serie di requisiti rigorosi, tra cui:

- **Sistema di gestione dei rischi (Articolo 9):** Un processo iterativo continuo per identificare, stimare e mitigare i rischi per salute, sicurezza e diritti fondamentali. Deve essere documentato, riesaminato e aggiornato. Le misure devono ridurre i rischi residui a un livello accettabile. I sistemi devono essere testati.
- **Qualità dei set di dati (Articolo 10):** I set di dati di training, validazione e test devono essere pertinenti, sufficientemente rappresentativi, privi di errori e completi. Devono considerare le caratteristiche geografiche, contestuali, comportamentali o funzionali dell'uso previsto. Il trattamento di categorie particolari di dati personali per rilevare e correggere bias è permesso in via eccezionale con garanzie rigorose.
- **Documentazione tecnica (Articolo 11):** Deve essere redatta e mantenuta aggiornata per dimostrare la conformità ai requisiti e fornire informazioni chiare alle autorità. Deve includere dettagli su progettazione, sviluppo, dati utilizzati, procedure di test, sistema di gestione dei rischi, ecc.
- **Conservazione delle registrazioni ("Log") (Articolo 12):** I sistemi devono consentire la registrazione automatica degli eventi per tutta la loro vita utile, al fine di individuare situazioni di rischio, facilitare il monitoraggio post-immissione sul mercato e monitorare il funzionamento.
- **Trasparenza e fornitura di informazioni ai deployer (Articolo 13):** I sistemi devono essere sufficientemente trasparenti da consentire ai deployer di interpretare l'output. Devono essere accompagnati da istruzioni per l'uso concise, complete, corrette e chiare, comprese informazioni sulle capacità, limitazioni, accuratezza, sicurezza, usi previsti e vietati, misure di sorveglianza umana, ecc.
- **Sorveglianza umana (Articolo 14):** I sistemi devono essere progettati per consentire un'efficace sorveglianza umana, che deve consentire ai deployer di monitorare il funzionamento, evitare un affidamento eccessivo, interpretare correttamente l'output, decidere di non utilizzare il sistema o ignorarne/annullarne l'output, e intervenire o arrestare il sistema in modo sicuro. Per i sistemi di identificazione biometrica ad alto rischio, l'identificazione deve essere verificata e confermata separatamente da almeno due persone fisiche, salvo eccezioni specifiche per le forze dell'ordine.
- **Accuratezza, robustezza e cibersecurity (Articolo 15):** I sistemi devono raggiungere un adeguato livello di accuratezza, robustezza e cibersecurity per tutto il loro ciclo di vita. Devono essere resilienti a errori, guasti e attacchi informatici (es. data poisoning, attacchi antagonisti). I livelli di accuratezza e le metriche pertinenti devono essere dichiarati nelle istruzioni per l'uso.

8. Obblighi degli Operatori (Sezione 3, Capo III)

Il regolamento specifica obblighi per diversi operatori nella catena del valore dell'IA:

- **Fornitori (Articolo 16):** Responsabili di garantire la conformità del sistema di IA ad alto rischio ai requisiti, implementare il sistema di gestione della qualità, conservare la documentazione, condurre la valutazione di conformità, applicare misure correttive e cooperare con le autorità.
- **Rappresentanti autorizzati (Articolo 22):** Per i fornitori stabiliti in paesi terzi, agiscono come punto di contatto nell'UE, verificano la documentazione e la conformità, e cooperano con le autorità.
- **Importatori (Articolo 23):** Devono garantire che i sistemi di IA ad alto rischio che immettono sul mercato siano conformi, verificando la valutazione di conformità del fornitore, il marchio CE e le informazioni richieste.
- **Distributori (Articolo 24):** Devono verificare che il sistema di IA ad alto rischio sia conforme al regolamento prima di metterlo a disposizione sul mercato.
- **Responsabilità lungo la catena del valore (Articolo 25):** Distributori, importatori o terzi sono considerati fornitori se appongono il proprio nome/marchio, apportano modifiche sostanziali a un sistema di IA ad alto rischio, o modificano la finalità prevista di un sistema di IA rendendolo ad alto rischio.
- **Deployer (Utilizzatori) (Articolo 26):** Devono utilizzare i sistemi di IA ad alto rischio in conformità con le istruzioni per l'uso, garantire la sorveglianza umana, utilizzare dati di input pertinenti, monitorare il funzionamento, conservare i log, e informare i lavoratori e le persone fisiche interessate.

9. Valutazione d'Impatto sui Diritti Fondamentali (Articolo 27)

I deployer di sistemi di IA ad alto rischio che sono organismi di diritto pubblico o enti privati che forniscono servizi pubblici (e altri specifici sistemi di cui all'Allegato III, punto 2) devono effettuare una **valutazione d'impatto sui diritti fondamentali** prima dell'uso. Questa valutazione deve identificare i rischi specifici per le persone o i gruppi, le misure di mitigazione, e deve essere notificata all'autorità di vigilanza del mercato. Se del caso, si integra con la valutazione d'impatto sulla protezione dei dati (GDPR).

10. Autorità di Notifica e Organismi Notificati (Sezione 4, Capo III)

- Ogni Stato membro designa almeno un'**autorità di notifica** responsabile della valutazione, designazione e monitoraggio degli **organismi di valutazione della conformità**.
- Gli organismi di valutazione della conformità, se conformi ai requisiti (indipendenza, competenza, assenza di conflitti di interesse, requisiti di cibersicurezza), possono essere **notificati** dalla Commissione e dagli altri Stati membri. (Articoli 28-31)
- Questi organismi notificati verificano la conformità dei sistemi di IA ad alto rischio. (Articolo 34)

11. Valutazione della Conformità, Certificati e Registrazione (Sezione 5, Capo III)

- I fornitori di sistemi di IA ad alto rischio devono seguire procedure di **valutazione della conformità** (controllo interno o valutazione del sistema di gestione della qualità con organismo notificato). (Articolo 43)
- I sistemi che si presumono ad alto rischio a causa dell'Allegato III, punti 2-8, seguono la procedura di controllo interno. I sistemi biometrici ad alto rischio (Allegato III, punto 1) generalmente richiedono il coinvolgimento di un organismo notificato.
- I sistemi di IA ad alto rischio che sono componenti di sicurezza di prodotti soggetti ad altra normativa UE (Allegato I, Sezione A) seguono le procedure di valutazione della conformità previste da tali atti.
- In caso di **modifica sostanziale** a un sistema di IA ad alto rischio, è richiesta una nuova valutazione di conformità. (Articolo 43, Paragrafo 4)
- I certificati rilasciati dagli organismi notificati hanno una validità limitata (es. 5 anni per sistemi Allegato I, 4 anni per Allegato III). (Articolo 44)
- I fornitori devono redigere una **dichiarazione di conformità UE** e apporre la **marcatore CE** sui sistemi di IA ad alto rischio conformi. (Articoli 47-48)
- I fornitori di sistemi di IA ad alto rischio (tranne quelli legati a prodotti Allegato I) e i deployer pubblici devono **registrarsi e registrare informazioni** sul loro sistema in una **banca dati dell'UE** gestita dalla Commissione. Questa banca dati è accessibile al pubblico, salvo per i sistemi utilizzati da forze dell'ordine, migrazione, asilo e controllo delle frontiere, che sono in una sezione non pubblica sicura. (Articolo 49, Articolo 71)

12. Obblighi di Trasparenza per Determinati Sistemi di IA (Articolo 50)

Il regolamento impone obblighi di trasparenza per i sistemi di IA che, pur non essendo necessariamente ad alto rischio, possono avere un impatto:

- **Interazione con persone fisiche:** I fornitori devono garantire che le persone siano informate che stanno interagendo con un sistema di IA, a meno che non sia evidente. (Articolo 50, Paragrafo 1)
- **Contenuti generati o manipolati artificialmente (Deep Fakes):** I fornitori di sistemi di IA (inclusi i modelli di IA per finalità generali) che generano contenuti sintetici (audio, immagine, video, testo) devono garantire che gli output siano **marcati in un formato leggibile meccanicamente e rilevabili come artificiali**. Le soluzioni tecniche devono essere efficaci, interoperabili, robuste e affidabili. Non si applica

a funzioni di editing standard o quando la modifica non è sostanziale, o se autorizzato dalla legge per scopi di forze dell'ordine. (Articolo 50, Paragrafo 2)

- **Sistemi di riconoscimento delle emozioni o di categorizzazione biometrica:** I deployer devono informare le persone esposte al loro funzionamento e trattare i dati personali in conformità con le normative sulla protezione dei dati. (Articolo 50, Paragrafo 3)
- **Deep Fakes da deployer:** I deployer che utilizzano un sistema di IA per generare o manipolare immagini, audio o video che assomigliano a persone, oggetti, luoghi o eventi esistenti, rendendoli falsamente autentici, devono **dichiarare chiaramente e distintamente che il contenuto è stato creato o manipolato artificialmente.** (Articolo 50, Paragrafo 4)

13. Modelli di IA per Finalità Generali (Capo V)

Il regolamento introduce regole specifiche per i modelli di IA per finalità generali (General Purpose AI Models - GPAI), in particolare quelli con "rischio sistemico".

- **Definizione (Articolo 3, Punto 63):** Un modello di IA, anche se addestrato con grandi quantità di dati usando l'autosupervisione su larga scala, caratterizzato da "generalità significativa" e capace di svolgere un'ampia gamma di compiti distinti, e che può essere integrato in vari sistemi a valle.
- **Classificazione a rischio sistemico (Articolo 51):** Un modello GPAI è classificato come a rischio sistemico se:
 - Presenta "capacità di impatto elevato" (valutate con strumenti tecnici e benchmark).
 - Soddisfa una soglia computazionale specifica (presunto se la quantità cumulativa di calcolo per il training supera 10^{25} operazioni in virgola mobile).
 - La Commissione lo designa tale sulla base di una valutazione che considera criteri come qualità/dimensione del dataset, input/output, livello di autonomia e scalabilità, impatto sul mercato interno (es. più di 10.000 utenti commerciali registrati nell'UE).
- **Obblighi per i fornitori di GPAI (Articolo 53):** Devono garantire la conformità al copyright, produrre e mantenere aggiornata la documentazione tecnica del modello (Allegato XI), e fornire informazioni chiare ai fornitori a valle (Allegato XII). Devono anche istituire una politica per il rispetto della legge sul diritto d'autore, in particolare riguardo all'estrazione di testo e dati dai contenuti utilizzati per il training.
- **Obblighi aggiuntivi per i fornitori di GPAI a rischio sistemico (Articolo 55):** Oltre agli obblighi sopra, devono:
 - Effettuare una valutazione dei modelli (es. test contraddittorio/adversarial testing) per identificare e mitigare i rischi sistemici.
 - Valutare e mitigare continuamente i rischi sistemici.
 - Monitorare, documentare e segnalare senza indebito ritardo incidenti gravi all'Ufficio per l'IA.
 - Garantire un adeguato livello di protezione della cibersicurezza per il modello e la sua infrastruttura fisica.
- **Codici di buone pratiche (Articolo 56):** L'Ufficio per l'IA e il comitato incoraggiano lo sviluppo di codici di buone pratiche per facilitare l'applicazione di questi obblighi, inclusi dettagli su come garantire la trasparenza, identificare e gestire i rischi sistemici.

14. Misure a Sostegno dell'Innovazione (Capo VI)

Il regolamento include misure per promuovere l'innovazione, in particolare per le PMI e le start-up:

- **Spazi di sperimentazione normativa per l'IA (AI Regulatory Sandboxes) (Articoli 57-59):** Quadranti controllati creati dalle autorità competenti che offrono a fornitori o potenziali fornitori la possibilità di sviluppare, addestrare, convalidare e testare sistemi di IA innovativi, anche in condizioni reali, sotto supervisione normativa. L'obiettivo è promuovere l'innovazione, rafforzare la certezza del diritto, facilitare l'apprendimento normativo e accelerare l'accesso al mercato. L'accesso dovrebbe essere prioritario per le PMI e le start-up e gratuito per esse.
- **Prove in condizioni reali al di fuori degli spazi di sperimentazione (Articoli 60-61):** Possono essere effettuate dai fornitori o potenziali fornitori di sistemi di IA ad alto rischio dell'Allegato III, previa

approvazione dell'autorità di vigilanza del mercato, informando i soggetti delle prove e ottenendone il consenso informato. Esistono garanzie procedurali e per la protezione dei dati.

- **Misure per PMI e start-up (Articolo 62):** Gli Stati membri devono fornire accesso prioritario agli spazi di sperimentazione, organizzare attività di sensibilizzazione e formazione, e facilitare la partecipazione al processo di normazione. Le tariffe per la valutazione della conformità devono tenere conto degli interessi delle PMI.
- **Deroghe per microimprese (Articolo 63):** Le microimprese possono conformarsi a determinati elementi del sistema di gestione della qualità in modo semplificato.

15. Governance (Capo VII)

Viene istituito un quadro di governance a livello dell'Unione:

- **Ufficio per l'IA (Articolo 64):** Creato dalla Commissione per sviluppare competenze e capacità dell'Unione nel settore dell'IA e contribuire all'attuazione del regolamento.
- **Comitato Europeo per l'Intelligenza Artificiale (Articolo 65):** Composto da rappresentanti degli Stati membri, fornisce consulenza e assistenza alla Commissione e agli Stati membri per un'applicazione coerente ed efficace del regolamento. Ha sottogruppi permanenti per la vigilanza del mercato e gli organismi notificati.
- **Forum Consultivo (Articolo 67):** Fornisce consulenza e competenze tecniche al Comitato e alla Commissione, con una composizione equilibrata di portatori di interessi (industria, start-up, PMI, società civile, mondo accademico, agenzie UE).
- **Gruppo di Esperti Scientifici Indipendenti (Articolo 68):** Sostiene l'Ufficio per l'IA nelle attività di esecuzione, in particolare per il monitoraggio dei modelli di IA per finalità generali e per segnalare rischi sistemici.
- **Autorità nazionali competenti (Articolo 70):** Ogni Stato membro deve designare almeno un'autorità di notifica e un'autorità di vigilanza del mercato. Devono disporre di risorse tecniche, finanziarie e umane adeguate e operare in modo indipendente e imparziale. Un'autorità di vigilanza del mercato funge da punto di contatto unico.

16. Vigilanza del Mercato ed Esecuzione (Capo IX)

- Il regolamento (UE) 2019/1020 sulla vigilanza del mercato si applica ai sistemi di IA. (Articolo 74)
- **Monitoraggio successivo all'immissione sul mercato (Articolo 72):** I fornitori devono istituire e documentare un sistema per monitorare i sistemi di IA ad alto rischio dopo la loro immissione sul mercato, inclusa l'analisi dell'interazione con altri sistemi.
- **Comunicazione di incidenti gravi (Articolo 73):** I fornitori devono segnalare immediatamente incidenti gravi alle autorità di vigilanza del mercato.
- **Accesso al codice sorgente (Articolo 74, Paragrafo 13):** Le autorità di vigilanza del mercato possono accedere al codice sorgente dei sistemi di IA ad alto rischio su richiesta motivata, se necessario e dopo aver esaurito altri mezzi di verifica.
- **Riservatezza (Articolo 78):** Tutte le parti coinvolte nell'applicazione del regolamento devono garantire la riservatezza delle informazioni ottenute, tutelando la proprietà intellettuale, i segreti commerciali, gli interessi di sicurezza nazionale, ecc.
- **Sanzioni (Articolo 99):** Sono previste sanzioni amministrative pecuniarie elevate per le violazioni, con importi massimi specifici per diverse categorie di infrazioni (es. fino a 35.000.000 EUR o 7% del fatturato annuo mondiale per le pratiche vietate). Le sanzioni devono essere effettive, proporzionate e dissuasive.

17. Diritti degli Individui (Sezione 4, Capo IX)

- **Diritto di presentare un reclamo (Articolo 85):** Qualsiasi persona fisica o giuridica può presentare un reclamo all'autorità di vigilanza del mercato competente in caso di violazione del regolamento.
- **Diritto alla spiegazione dei singoli processi decisionali (Articolo 86):** Le persone hanno il diritto di ottenere una spiegazione quando una decisione che produce effetti giuridici negativi su di esse si basa principalmente sugli output di determinati sistemi di IA ad alto rischio.
- **Protezione degli informatori (Articolo 87):** La Direttiva (UE) 2019/1937 si applica alla segnalazione di violazioni del presente regolamento e alla protezione delle persone che segnalano tali violazioni.

18. Esecuzione degli Obblighi per i Fornitori di Modelli di IA per Finalità Generali

(Sezione 5, Capo IX)

- La **Commissione (tramite l'Ufficio per l'IA)** ha competenze esclusive per la vigilanza e l'esecuzione degli obblighi dei fornitori di modelli di IA per finalità generali (Capo V). (Articolo 88)
- L'Ufficio per l'IA può svolgere **azioni di monitoraggio**, richiedere documentazione e informazioni, ed effettuare valutazioni dei modelli, compreso l'accesso al codice sorgente. (Articoli 89-92)
- La Commissione può **richiedere misure** ai fornitori, inclusa l'adozione di misure correttive o la limitazione della messa a disposizione sul mercato, il ritiro o il richiamo del modello. (Articolo 93)

19. Disposizioni Finali e Tempistiche

- Il regolamento entra in vigore 20 giorni dopo la pubblicazione nella Gazzetta Ufficiale dell'Unione Europea.
- Si applica generalmente 24 mesi dopo l'entrata in vigore.
- Tuttavia, alcune disposizioni hanno tempistiche di applicazione anticipate:
- **6 mesi dopo l'entrata in vigore:** Capi I (Disposizioni Generali) e II (Pratiche di IA Vietate).
- **12 mesi dopo l'entrata in vigore:** Capo III, Sezione 4 (Autorità di Notifica e Organismi Notificati), Capo V (Modelli di IA per Finalità Generali), Capo VII (Governance), Capo XII (Sanzioni - tranne Articolo 101), e Articolo 78 (Riservatezza).
- **36 mesi dopo l'entrata in vigore:** Articolo 6, Paragrafo 1 (IA ad alto rischio come componenti di prodotto).
- I fornitori di sistemi di IA ad alto rischio e i deployer pubblici devono conformarsi entro specifici periodi transitori (es. fine 2030 per sistemi IT su larga scala, 6 anni per sistemi IA usati da autorità pubbliche).

Questo regolamento rappresenta un passo significativo per l'UE nel creare un quadro giuridico solido e coerente per l'IA, bilanciando l'innovazione con la protezione dei diritti fondamentali e la sicurezza.