

Il Regolamento Europeo sull'Intelligenza Artificiale

Un Quadro Normativo Completo per la Governance dell'IA

Prof. Fedeli Massimo - Tutti i diritti riservati

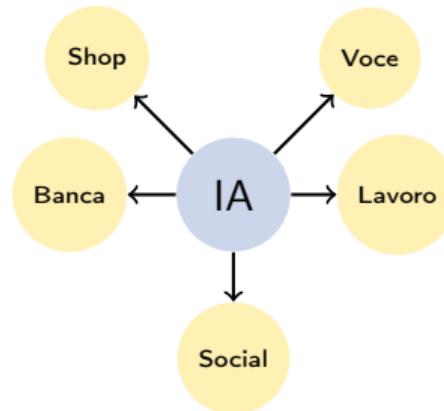
IIS Fermi Sacconi Cpiia- Ascoli Piceno

6 gennaio 2026

La Rivoluzione dell'IA nella Vita Quotidiana

L'IA è ovunque:

- Raccomandazioni e suggerimenti online
- Assistenti vocali sugli smartphone
- Sistemi di valutazione del credito
- Screening di CV per candidature
- Filtraggio contenuti sui social media



La necessità di regolamentazione:

- Proteggere i diritti fondamentali
- Garantire sicurezza e trasparenza
- Bilanciare innovazione e protezione

Tappe Fondamentali

- **9 dicembre 2023:** Accordo provvisorio raggiunto
- **Primo al mondo:** Quadro normativo completo sull'IA
- **Legislazione storica:** Stabilisce standard globali per la governance dell'IA

Cosa definisce:

- Cosa si può e non si può fare con l'IA
- Garanzie per i cittadini
- Responsabilità delle aziende

Chi riguarda:

- Sviluppatori e fornitori di IA
- Aziende che utilizzano sistemi IA
- Istituzioni pubbliche
- Cittadini e utenti finali

Il principio fondamentale:

"Maggiore rischio = Regole più stringenti"



Trovare l'equilibrio tra protezione e innovazione

Rischio Inaccettabile: Pratiche IA Vietate

Queste applicazioni IA sono completamente vietate nell'UE:

① Sistemi di manipolazione comportamentale

- Sfruttamento di vulnerabilità (età, disabilità, status economico)
- Tecniche subliminali o ingannevoli

② Sistemi di social scoring

- Valutazione dei cittadini in base a comportamento o caratteristiche
- Sorveglianza sociale di massa da enti pubblici o privati

③ Categorizzazione biometrica basata su dati sensibili

- Inferire razza, opinioni politiche, orientamento sessuale
- Dedurre convinzioni religiose o filosofiche

Principio

Queste pratiche sono incompatibili con i valori fondamentali dell'UE e la Carta dei Diritti Fondamentali.



Altre Pratiche Vietate

4. Riconoscimento delle Emozioni

Vietato in:

- Ambienti di lavoro
- Istituzioni educative

Eccezione:

- Scopi medici e di sicurezza
- Esempio: monitoraggio affaticamento piloti

5. Raccolta di Immagini Facciali

- Raccolta non mirata da internet
- Da sistemi CCTV
- Per creare/espandere database di riconoscimento facciale

Altre pratiche vietate

6. Riconoscimento Facciale in Tempo Reale

Divieto generale per le forze dell'ordine negli spazi pubblici

Eccezioni limitate:

- Ricerca mirata di vittime
- Prevenzione di minacce specifiche
- Rilevamento crimini gravi

Richiede autorizzazione giudiziaria e supervisione rigorosa



Esempio Concreto: Divieto di Riconoscimento delle Emozioni

Scenario Vietato

L'azienda X installa telecamere per rilevare emozioni

- Monitora espressioni facciali dei dipendenti
- Analizza “livelli di coinvolgimento” durante riunioni
- Usa i dati per valutazioni delle prestazioni
- Afferma di rilevare “stress” o “felicità”

Risultato: VIETATO dall'AI Act

Esempio Scolastico

Università installa IA per rilevare attenzione studenti

- Telecamere analizzano espressioni facciali
- Sistema segnala studenti “distratti”
- Dati condivisi con professori
- Influenza voti di partecipazione

Risultato: VIETATO

Esempio concreto

Perché è Vietato

- Invade la privacy dei lavoratori
- Rilevamento emozioni inaffidabile
- Crea pressione psicologica
- Potenziale di discriminazione

Eccezione Consentita

Sistema di monitoraggio ospedaliero:

- Rileva livelli di stress del paziente
- Scopo di sicurezza medica
- Supervisione di professionisti sanitari
- Richiesto consenso del paziente

Risultato: CONSENTITO

Esempio Concreto: Sistemi di Social Scoring

Scenario Vietato: Sistema “Punteggio Sociale”

Un governo comunale implementa un sistema IA di punteggio:

- Traccia attività sui social media, abitudini di acquisto, connessioni sociali dei cittadini
- Assegna a ogni persona un punteggio da 0 a 1000
- Punteggi alti: accesso prioritario ad alloggi pubblici, permessi più rapidi
- Punteggi bassi: restrizioni sui servizi, tariffe assicurative più alte
- Sistema penalizza post “negativi” sui social o associazioni con chi ha punteggi bassi

Risultato: ASSOLUTAMENTE VIETATO

Esempio concreto: Sistemi di Social Scoring

Perché è Vietato

- Sorveglianza di massa
- Accesso discriminatorio ai servizi
- Blocca la libera espressione
- Viola la dignità umana
- Crea controllo sociale

Contesto Reale

- Sistema di Credito Sociale cinese
- Milioni di persone colpite
- Restringe viaggi, lavoro, servizi
- Basato su monitoraggio comportamenti

Tali scenari distopici non possono essere implementati nell'UE

Esempi Concreti: Violazioni Biometriche

Vietato: Categorizzazione Biometrica

Scenario: Sistema di “Sicurezza” Aeroportuale

- IA analizza caratteristiche facciali dei passeggeri
- Tenta di inferire etnia o credenze religiose
- Segnala certi profili per controlli aggiuntivi
- Nessuna prova, solo basato sull'aspetto

Impatto nel Mondo Reale

Caso di Studio: Clearview AI

- Azienda USA ha raccolto oltre 3 miliardi di immagini
- Creato database di riconoscimento facciale
- Venduto alle forze dell'ordine
- Vari paesi UE l'hanno multata
- **L'AI Act vieterebbe esplicitamente questo**

Esempi concreti: violazioni biometriche

Vietato: Raccolta Facciale

Scenario: Database di Azienda Tecnologica

- Raccoglie miliardi di foto dai social media
- Costruisce database di riconoscimento facciale
- Vende accesso ad aziende private
- Nessun consenso degli utenti ottenuto

Risultato: VIETATO

Il Danno

- Viola la privacy su scala massiva
- Abilita la discriminazione
- Nessun controllo individuale

Sistemi IA ad Alto Rischio: Quando l'IA Richiede Garanzie Speciali



Non vietati, ma soggetti a obblighi rigorosi

Requisiti Chiave

- Valutazione di conformità prima dell'immissione sul mercato
- Dati di qualità per l'addestramento
- Documentazione tecnica
- Trasparenza del funzionamento
- Capacità di supervisione umana
- Accuratezza e robustezza

Principio Principale

I sistemi possono essere usati solo se rispettano standard di qualità, sicurezza e trasparenza

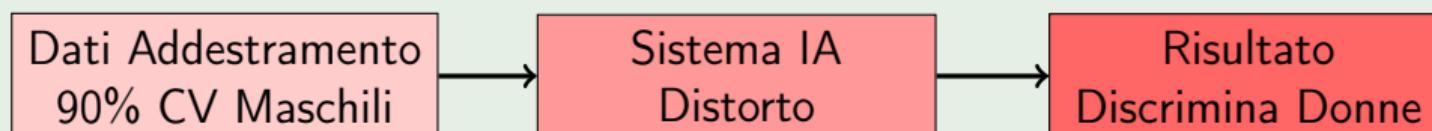
Requisiti

Valutazione

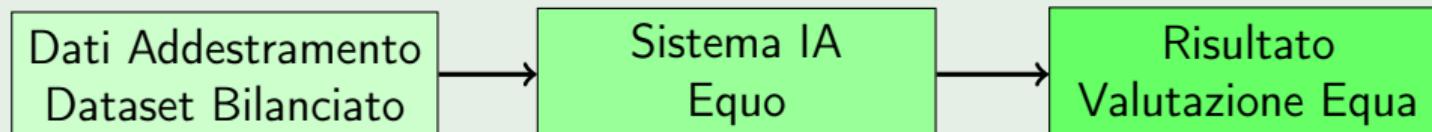
Qualità dei Dati: Combattere la Discriminazione

I sistemi ad alto rischio devono essere addestrati con dataset rappresentativi

Example (Problema: Sistema di Reclutamento Distorto)



Soluzione: Addestramento Rappresentativo



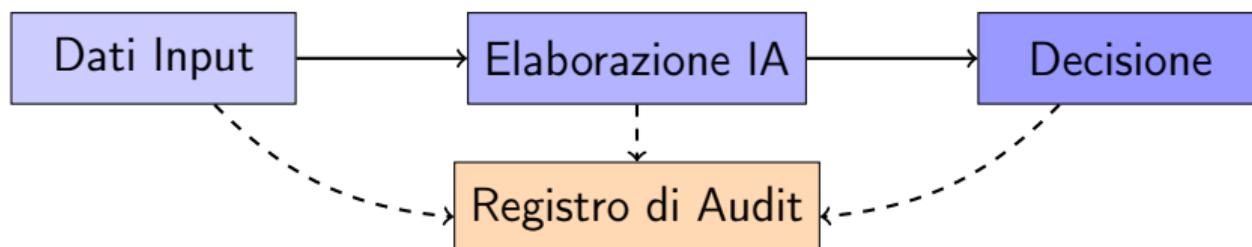
Il regolamento richiede l'identificazione e la mitigazione dei rischi di

Tracciabilità: Comprendere le Decisioni dell'IA

Perché la Tracciabilità è Importante

I sistemi ad alto rischio devono essere tracciabili per ricostruire:

- Come il sistema è arrivato a una decisione
- Quali dati sono stati utilizzati
- Come il sistema è stato addestrato



Documentazione completa permette verifica e indagine

Sistemi ad Alto Rischio: Categorie Pratiche (1/3)

1. Identificazione Biometrica

- Sistemi biometrici per identificare persone
- Quando non completamente vietati
- Richiesta supervisione rigorosa

2. Infrastrutture Critiche

- Reti elettriche, acqua, gas
- Gestione traffico stradale
- Sistemi il cui guasto può impattare la sicurezza

Nota Importante

Queste categorie riguardano sistemi che possono avere impatto diretto sulla sicurezza fisica e l'identificazione delle persone

Sistemi ad Alto Rischio: Categorie Pratiche (2/3)

3. Istruzione

- Determinazione accesso alle istituzioni educative
- Valutazione risultati di apprendimento degli studenti
- Monitoraggio per disonestà negli esami
- Sistemi che influenzano il percorso formativo

Esempi Pratici

- Algoritmi per ammissione universitaria
- Sistemi di valutazione automatica
- Software di proctoring online

Sistemi ad Alto Rischio: Categorie Pratiche (3/3)

4. Occupazione e Gestione dei Lavoratori

- Sistemi di screening e selezione CV
- Valutazione automatica di colloqui
- Monitoraggio delle prestazioni lavorative
- Decisioni su promozioni e licenziamenti

Filo Conduttore delle Categorie

Tutti questi sistemi possono influenzare significativamente i diritti fondamentali, le opportunità di vita e la sicurezza delle persone

Sistemi ad Alto Rischio: Categorie Pratiche (Altre Categorie)

5. Servizi Essenziali

- Accesso a prestazioni pubbliche
- Accesso all'assistenza sanitaria
- Idoneità al welfare sociale
- Invio servizi di emergenza

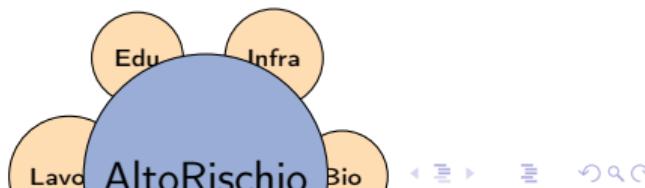
6. Servizi Finanziari

- Sistemi di credit scoring
- Valutazione affidabilità creditizia
- Calcolo premi assicurativi
- Decisioni approvazione prestiti

7. Giustizia e Legge (Richiesta Italiana)

- Assistenza ai giudici nella ricerca
- Interpretazione di fatti e legge
- Risoluzione alternativa controversie

L'Italia ha sostenuto con successo l'inclusione dei sistemi IA giudiziari

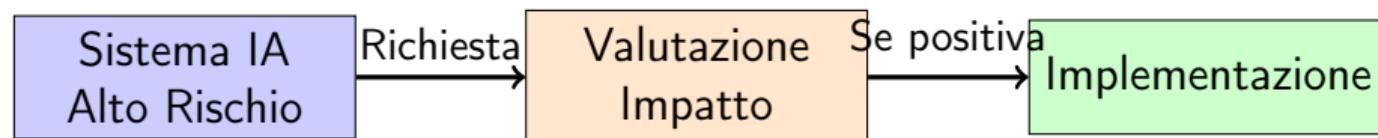


Valutazione d'Impatto sui Diritti Fondamentali

Obbligo aggiuntivo per enti pubblici e fornitori di servizi pubblici

La Valutazione Deve Descrivere:

- ① Come verrà utilizzato il sistema
- ② Chi ne sarà interessato
- ③ Quali rischi esistono
- ④ Quali misure di mitigazione sono state adottate



Obbligatoria per PA che usa IA ad alto rischio

Rischio Minimo: La Maggioranza dei Sistemi IA (1/2)



La maggior parte dei sistemi IA attualmente usati nell'UE rientra in questa categoria

Esempi di Applicazioni

- Videogiochi con IA
- Filtri antispam email
- Raccomandazioni per acquisti online
- Assistenti virtuali semplici
- Molte applicazioni quotidiane
- Strumenti di editing foto/video

Caratteristiche Comuni

- Impatto limitato sui diritti fondamentali
- Rischi minimi per gli utenti
- Utilizzo diffuso e consolidato
- Benefici chiari per i consumatori

Rischio Minimo: La Maggioranza dei Sistemi IA (2/2)

Requisiti Regolatori

- **Nessun obbligo speciale**
- Nessuna valutazione di conformità richiesta
- Nessuna burocrazia complessa
- Libero sviluppo e implementazione

Integrazione con Altra Normativa

Sistemi già regolati da:

- Digital Services Act (DSA)
- Digital Markets Act (DMA)
- GDPR (protezione dati)
- Normative settoriali esistenti

Nessuna sovrapposizione normativa

Misure Volontarie Incoraggiate

- Adozione di codici di condotta
- Implementazione di best practice
- Autoregolamentazione settoriale

Vantaggi dell'Approccio

- Riduzione oneri amministrativi

Gli utenti devono essere informati quando interagiscono con l'IA

1. Chatbot e Assistenti Virtuali

Richiesta divulgazione chiara:

- L'utente sta interagendo con una macchina
- Non con una persona reale
- Previene l'inganno

2. Contenuti Generati da IA

Devono essere chiaramente etichettati:

- Testi generati da IA
- Immagini create da IA
- Audio sintetizzato da IA
- Video prodotti da IA

Example (Buona Pratica)

"Ciao! Sono un assistente IA. Come posso aiutarti oggi?"

Formato Leggibile da Macchine

- Etichettatura facilmente rilevabile
- Verifica automatica possibile

La Sfida dei Deepfake

Cosa sono i Deepfake?

Video o audio manipolati che fanno sembrare che una persona abbia detto o fatto cose che non ha mai fatto realmente

Rischi

- Diffusione disinformazione
- Danno alla reputazione
- Manipolazione politica
- Frode d'identità
- Erosione della fiducia

Requisiti del Regolamento

I deepfake devono essere:

- Esplicitamente divulgati come tali
- Chiaramente etichettati
- Identificabili dagli utenti
- Tracciabili alla fonte

IA per Finalità Generali e Modelli Fondativi (1/2)

Una nuova categoria aggiunta durante i negoziati (su insistenza del Parlamento)

Cosa sono i Modelli IA per Finalità Generali?

Sistemi capaci di svolgere un'ampia varietà di compiti:

- Generare testo, immagini, codice
- Tradurre lingue
- Rispondere a domande
- Analizzare dati

Esempi: GPT-4 (OpenAI), Gemini (Google), Claude (Anthropic)

Caratteristiche Distintive

- Versatilità: un solo modello per molteplici applicazioni
- Addestramento su enormi quantità di dati
- Capacità di apprendimento generalizzato
- Possibilità di essere adattati a compiti specifici (fine-tuning)

IA per Finalità Generali e Modelli Fondativi (2/2)

Differenza da IA a Scopo Specifico

IA Generica:

- Capacità multi-funzionali
- Ampia applicabilità
- Potenziali rischi sistematici
- Utilizzo imprevedibile

Perché Regolarli?

- Impatto su larga scala
- Potenziale di uso improprio
- Rischi a livello sociale
- Necessità di responsabilità
- Difficoltà nel prevedere tutti gli usi
- Possibile amplificazione di bias

IA Specifica

- Progettata per un compito
- Ambito limitato
- Rischi più prevedibili

Approccio Regolatorio

Focus sulla catena di valore: dal modello base all'applicazione finale

Modelli con Rischio Sistematico (1/2)

I modelli più potenti richiedono garanzie aggiuntive

Soglia di Identificazione

Modelli addestrati con potenza computazionale superiore a:

10^{25} FLOPS (Operazioni in Virgola Mobile al Secondo)

Questa soglia può essere aggiornata dall'Ufficio per l'IA man mano che la tecnologia evolve

Contesto

Si tratta di modelli di intelligenza artificiale estremamente potenti, come i grandi modelli linguistici (LLM) di ultima generazione, che per la loro capacità possono rappresentare rischi a livello di sistema

Modelli con Rischio Sistematico (2/2)

Rischi Sistemici Potenziali

- Disinformazione di massa
- Attacchi informatici coordinati
- Manipolazione sociale su larga scala
- Guasti con effetti diffusi
- Conseguenze indesiderate imprevedibili

Obblighi per i Provider

- Valutare i rischi sistematici
- Mitigare i rischi identificati
- Segnalare incidenti gravi
- Condurre test approfonditi
- Garantire cybersicurezza
- Riportare consumo energetico

Maggiore potenza = Maggiore responsabilità

Open Source: Bilanciare Innovazione e Sicurezza

Esenzioni Open Source

Il regolamento riconosce il valore di:

- Innovazione collaborativa
- Sviluppo open-source
- Avanzamento della ricerca
- Contributi della comunità

Benefici

Modelli gratuiti con codice aperto
possono beneficiare di requisiti più leggeri

Limitazione Importante

Anche i modelli open-source devono rispettare obblighi di sicurezza più rigorosi se raggiungono la soglia di rischio sistematico

L'Equilibrio

- Incoraggiare l'innovazione
- Proteggere dai rischi sistematici
- Supportare la comunità di ricerca
- Mantenere standard di sicurezza



Il regolamento sull'IA per Finalità Generali è stato molto controverso

Preoccupazioni Iniziali

Italia, Francia, Germania preoccupate per:

- Penalizzazione aziende europee
- Svantaggio competitivo vs USA/Cina
- Regolamentazione eccessiva che soffoca innovazione
- Costi di conformità

Il Compromesso

- Obblighi vincolanti per modelli più potenti
- Ruolo importante per autoregolamentazione tramite codici di condotta
- Flessibilità per l'innovazione
- Requisiti di sicurezza forti mantenuti

Sanzioni: Garantire la Conformità

Pesanti sanzioni per garantire il rispetto del regolamento

Struttura delle Sanzioni

Le sanzioni variano in base alla gravità della violazione e possono essere calcolate come:

- Importo fisso in milioni di euro, OPPURE
- Percentuale del fatturato annuo mondiale

Si applica l'importo maggiore

Più Gravi

Fino a €35M
o 7% fatturato

Gravi

Fino a €15M
o 3% fatturato

Altre

Fino a €7,5M
o 1,5% fatturato

IA vietata

Altri requisiti

◀ Informazioni false ▶ 🔍

Sanzioni: Disposizioni Speciali (1/2)

Trattamento per PMI e Startup

Protezione speciale:

- Si applica l'importo più basso tra i due
- Riconoscimento che multe elevate potrebbero essere devastanti
- Principio di proporzionalità e sostenibilità

Esempio Pratico

Per una PMI che viola i requisiti sui dati:

Razionale della Disposizione

- Supportare l'innovazione europea
- Evitare di soffocare le startup
- Mantenere competitività
- Bilanciare conformità e crescita economica

Chi Ne Beneficia

- Piccole e medie imprese (PMI)
- Startup tecnologiche
- Aziende in fase di crescita

Sanzioni: Disposizioni Speciali (2/2)

Istituzioni dell'Unione Europea

Nessuna esenzione:

- Agenzie e istituzioni UE soggette a multe
- Il Garante Europeo della Protezione Dati può imporre sanzioni
- Le regole si applicano equamente a pubblico e privato

Diritti dei Cittadini

- Diritto di presentare reclami alle autorità
- Autorità di vigilanza devono indagare
- Procedure specifiche garantite per legge
- Tutela effettiva dei diritti fondamentali

Principio Fondamentale

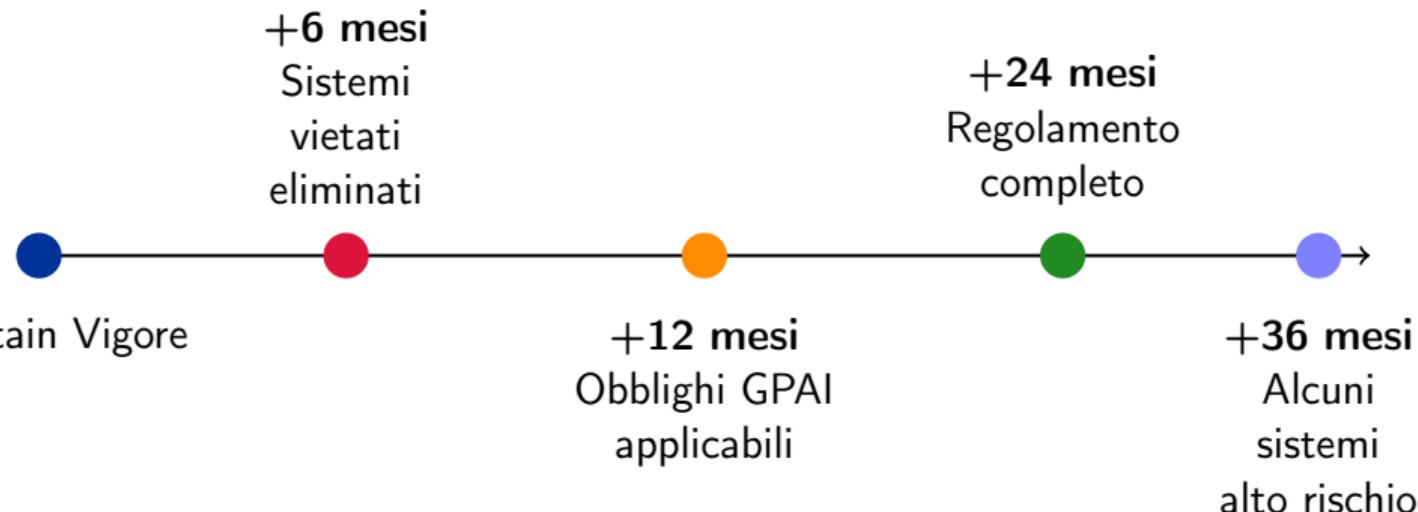
Accountability universale: nessuno è al di

Meccanismi di Enforcement

- Indagini obbligatorie

Quando Entrerà in Vigore?

Implementazione graduale per consentire tempo di preparazione



Un Modello per il Mondo?

L'Effetto Bruxelles: La regolamentazione UE influenza gli standard globali

Precedente: GDPR

Il regolamento UE sulla protezione dati è diventato uno standard de facto globale:

- Aziende si sono adattate globalmente
- Altri paesi hanno adottato leggi simili
- Stabiliti norme privacy mondiali

Potenziale AI Act

Potrebbe seguire lo stesso percorso:

- I giganti tech devono conformarsi per

Approcci Diversi

Stati Uniti:

- Orientato al mercato
- Meno interventista
- Regole settore-specifiche

Cina:

- Controllo centralizzato
- Orientamento al controllo sociale
- Sviluppo guidato dallo Stato

Domande Aperte e Sfide

Il regolamento è rivoluzionario, ma restano molte domande

① Evoluzione tecnologica

- Le regole rimarranno appropriate tra 5-10 anni?
- La regolamentazione può tenere il passo con lo sviluppo dell'IA?

② Equilibrio tra protezione e innovazione

- L'Europa rimarrà indietro nella corsa tecnologica globale?
- L'UE può favorire campioni dell'IA?

③ Efficacia dell'applicazione

- Le sanzioni saranno sufficientemente dissuasive?
- Le autorità hanno risorse ed expertise adeguate?

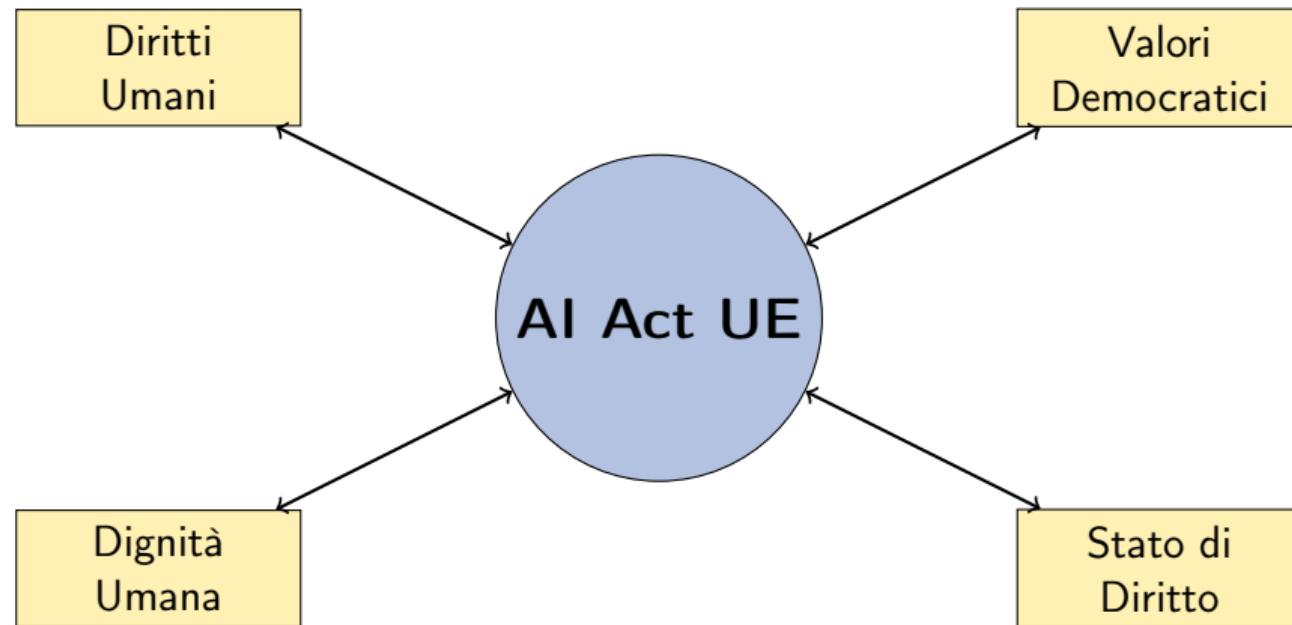
④ Coordinamento globale

- Altre grandi economie seguiranno l'esempio?
- Rischio di frammentazione normativa?

⑤ Implementazione pratica

Principi Fondamentali: La Scelta Europea

I valori fondamentali che guidano l'AI Act



Conclusione: Un Passo Storico

Risultati Chiave

- Prima regolamentazione IA completa al mondo
- Approccio basato sul rischio e proporzionato
- Regole chiare sulle pratiche vietate
- Forti garanzie per sistemi ad alto rischio
- Requisiti di trasparenza
- Regolamentazione modelli IA potenti
- Sanzioni significative

Guardando Avanti

- L'implementazione sarà critica
- Necessario monitoraggio
- Adattamento all'evoluzione tecnologica
- Cooperazione internazionale

IIS Fermi Sacconi Cpia
Ascoli Piceno, Italia

*Comprendere la Regolamentazione dell'IA
per un Futuro Digitale Migliore*