Il Regolamento Europeo sull'Intelligenza Artificiale

Un Quadro Normativo Completo per la Governance dell'IA

Prof. Fedeli Massimo - Tutti i diritti riservati

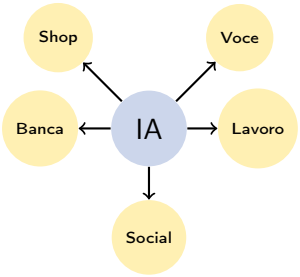
IIS Fermi Sacconi Cpia- Ascoli Piceno

5 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

L'AI Act: Un Traguardo Storico

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

Un Approccio Innovativo: Regolamentazione Basata sul Rischio

Il principio fondamentale:

"Maggiore rischio = Regole più stringenti"

Pochi obblighi

Requisiti rigorosi

VIETATO

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

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

Eccezione Consentita

Esempio Concreto: Sistemi di Social Scoring

Scenario Vietato: Sistema "PunteggioSociale"

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

Perché è Vietato

- Sorveglianza di massa

Contesto Reale

- Sistema di Credito Sociale cinese

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**

Il Danno

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

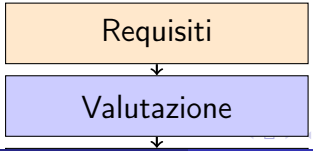
Non vietati, ma soggetti a obblighi rigorosi

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

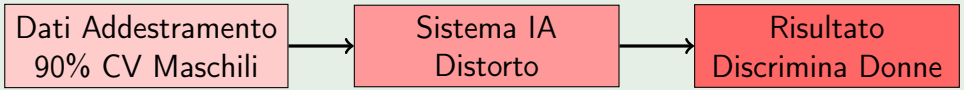
I sistemi possono essere usati solo se rispettano standard di qualità, sicurezza e trasparenza



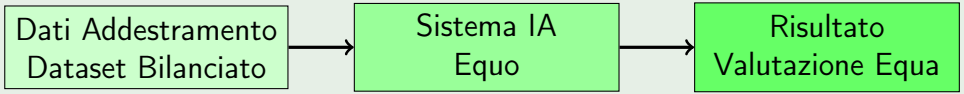
Qualità dei Dati: Combattere la Discriminazione

I sistemi ad alto rischio devono essere addestrati con dataset rappresentativi

Example (Problema: Sistema di Reclutamento Distorto)



Soluzione: Addestramento Rappresentativo



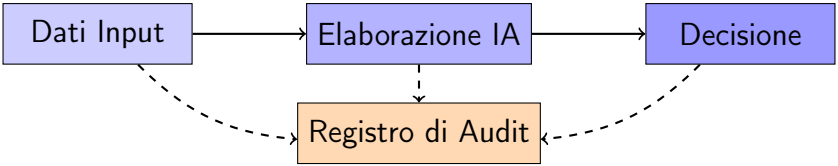
Il regolamento richiede l'identificazione e la mitigazione dei rischi di

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 (1/2)

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

4. Occupazione

- Sistemi di screening CV
- Valutazione colloqui
- Monitoraggio prestazioni
- Decisioni su promozioni e licenziamenti

Filo Conduttore

Tutti questi sistemi possono influenzare significativamente i diritti fondamentali e la sicurezza delle persone

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

5. Servizi Essenziali

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

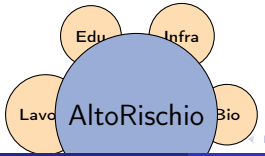
6. Servizi Finanziari

- 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

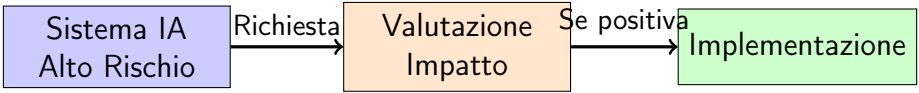


Valutazione d'Impatto sui Diritti Fondamentali

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

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

Esempi

- Videogiochi con IA
- Filtri antispam
- Raccomandazioni acquisti online
- Molte applicazioni quotidiane

Misure Volontarie

Adozione incoraggiata di:

- Codici di condotta
- Best practice
- Autoregolamentazione

Requisiti

- Nessun obbligo speciale

Integrazione

Sistemi già regolati da:

Trasparenza: Il Diritto di Sapere

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

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)

Differenza Chiave

Perché Regolarli?

Modelli con Rischio Sistemico

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

Rischi Sistemici

- Disinformazione di massa
- Attacchi informatici coordinati

Obblighi Richiesti

- Valutare i rischi sistemici
- Mitigare i rischi identificati

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 sistemico

L'Equilibrio

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

Il Percorso verso l'Accordo: I Negoziati

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	**Gravi**	**Altre**
Fino a €35M	Fino a €15M	Fino a €7,5M
o 7% fatturato	o 3% fatturato	o 1,5% fatturato
IA vietata	Altri requisiti	Informazioni false

Sanzioni: Disposizioni Speciali

PMI e Startup

Trattamento speciale:

- Si applica l'importo più basso dei due
- Riconoscimento che multe elevate potrebbero essere devastanti
- Principio di proporzionalità

Esempio

Per una PMI che viola i requisiti sui dati:

- €35M o 7% del fatturato
- **Importo più basso** viene applicato

Istituzioni UE

Nessuna esenzione:

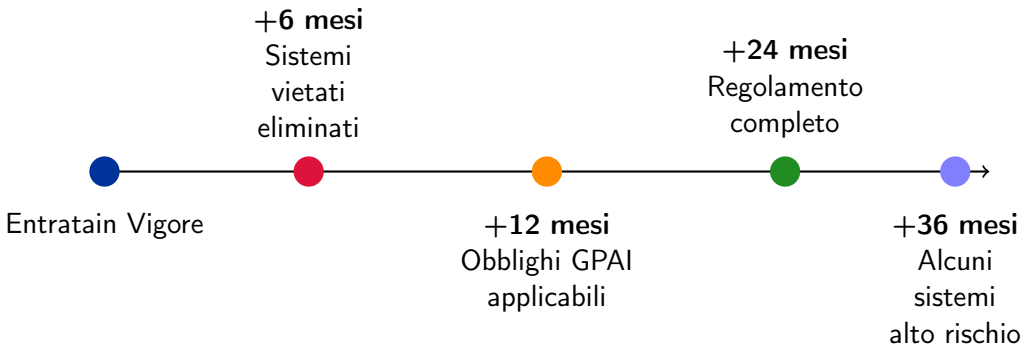
- Agenzie UE soggette a multe
- Il Garante Europeo della Protezione Dati può imporre sanzioni
- Le regole si applicano a pubblico e privato allo stesso modo

Diritti dei Cittadini

- Diritto di presentare reclami
- Autorità di vigilanza devono indagare
- Procedure specifiche garantite

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

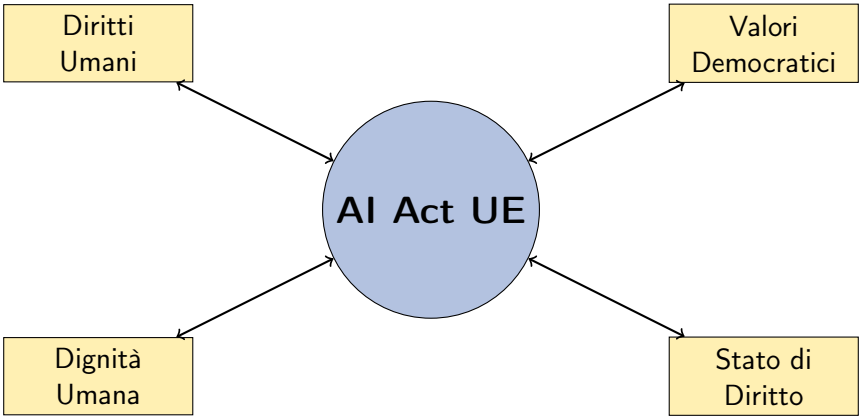
Domande Aperte e Sfide

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

La Sfida

Grazie!

Domande?

IIS Fermi Sacconi Ceci
Ascoli Piceno, Italia

Comprendere la Regolamentazione dell'IA
per un Futuro Digitale Migliore