Università degli Studi di Catania

Artificial Intelligence Act

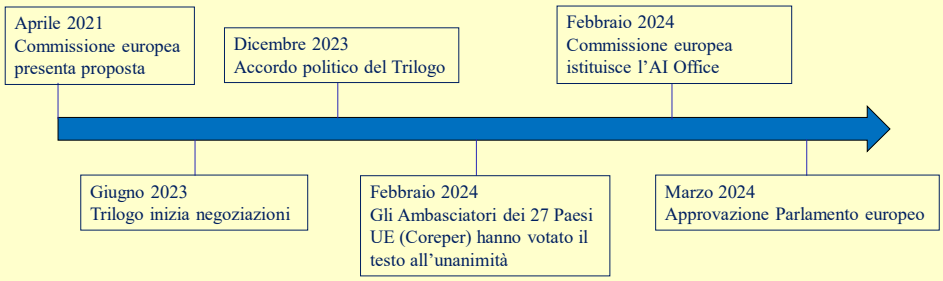
Seminario del corso di Digital forensics

Ignazio Zangara

Corso di laurea in Informatica

Anno accademico 2023/2024

AI Act ~ pietre miliari



L'AI Act è costituito da 113 Art., 180 Con. e 13 All.

La concreta applicazione è scadenzata dopo l'entrata in vigore:

- *i divieti relativi a pratiche vietate si applicheranno a partire da 6 mesi dopo (rischio inaccettabile)*
- *i codici di buone pratiche 9 mesi dopo*
- *le norme sui sistemi di IA per finalità generali (GPAI) 12 mesi dopo*
- *gli obblighi per i sistemi ad alto rischio 36 mesi dopo*

Visione

Tecnologia antropocentrica: "strumento per le persone con il fine ultimo di migliorare il benessere degli esseri umani" (Considerando 6)

Garantire la sicurezza e i diritti fondamentali delle persone e delle imprese e rafforzare la diffusione, gli investimenti e l'innovazione nell'UE

- ✓ *Europa come polo globale di eccellenza nell'IA, dal laboratorio al mercato*
- ✓ *Rispetto dei valori e delle regole consolidati*

Governance (1/2)

Ufficio sull'Intelligenza Artificiale (*AI Office*)

È responsabile dell'attuazione effettiva dell'AI Act, promuove l'uso di sistemi affidabili, monitora l'evoluzione del mercato di settore, coopera con le autorità e gli organismi dei singoli Stati membri

European Artificial Intelligence Board (*EAIB*)

Garantirà l'armonizzazione tra gli Stati membri nell'applicazione dell'AI ACT offrendo consulenza alla Commissione e agli Stati

Autorità nazionale per l'Intelligenza Artificiale

Ha il compito di irrogare le sanzioni previste in caso di violazioni (ruolo analogo a quello esercitato dal Garante della privacy). Dovrà esercitare i suoi poteri in modo indipendente, imparziale e senza pregiudizi, disponendo di risorse tecniche, finanziarie, umane, ed infrastrutture adeguate

Governance (2/2)

Forum consultivo

Formato da una selezione equilibrata di portatori di interesse, (industria, start-up, PMI, società civile e mondo accademico)
Ed inoltre, alcuni enti come l'Agenzia per i Diritti Fondamentali, l'Agenzia dell'Unione Europea per la Cybersecurity ed il Comitato Europeo di Normazione, quali membri permanenti

Comitato Scientifico di esperti indipendenti

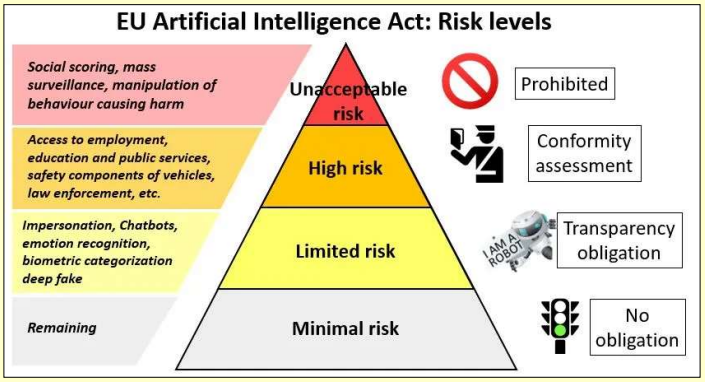
Fornirà consulenza e supporto all'AI Office, per quanto riguarda i modelli e i sistemi di IA ad uso generale

- *segnalando possibili rischi sistemici*
- *contribuendo allo sviluppo di strumenti e metodologie per valutare le capacità dei modelli e dei sistemi di IA ad uso generale*

Struttura

L'AI Act si basa su un sistema di classificazione per determinare il **livello di rischio** che una tecnologia basata sull'intelligenza artificiale potrebbe rappresentare **per la salute, la sicurezza o i diritti fondamentali delle persone**

Sono previsti quattro livelli di rischio:
inaccettabile, elevato, limitato e minimo



Applicazioni fuori legge → minacce ai diritti dei cittadini

• **Categorizzazione biometrica** basata su caratteristiche sensibili
• Estrapolazione indiscriminata di **immagini facciali** da internet o dalle registrazioni dei sistemi di telecamere a circuito chiuso **per creare banche dati** di riconoscimento facciale
• **Riconoscimento delle emozioni** sul luogo di lavoro e nelle scuole
• **Credito sociale**
• **Polizia predittiva** (se basate esclusivamente sulla profilazione o sulla valutazione delle caratteristiche di una persona)
• **Manipolazione del comportamento** umano o sfruttamento delle vulnerabilità delle persone

FORZE DELL'ORDINE
Le forze dell'ordine non potranno fare ricorso ai sistemi di identificazione biometrica, salvo i casi espressamente previsti dalla legge

L'identificazione "in tempo reale" potrà essere utilizzata solo se saranno rispettate garanzie rigorose, ad esempio se l'uso è limitato nel tempo e nello spazio e previa autorizzazione giudiziaria o amministrativa
Esempio: la ricerca di una persona scomparsa o la prevenzione di un attacco terroristico

Sistemi ad alto rischio

• Destinati a essere utilizzati come **componenti di sicurezza di prodotti** (o qualora i sistemi di IA siano essi stessi prodotti)
• Che rientrano in **settori critici**, se presentano un rischio significativo di danno per la salute umana, la sicurezza o i diritti fondamentali delle persone fisiche
- Es.: destinati ad essere utilizzati nei settori dell'istruzione, della sanità, della selezione del personale, della sicurezza, dell'amministrazione della giustizia e della pubblica amministrazione, qualora siano idonei a incidere sulla salute, sulla libertà e sui diritti fondamentali dei cittadini

Requisiti e obblighi per accedere al mercato dell'UE
• adozione di sistemi di gestione dei rischi
• elevata qualità dei set di dati che alimentano il sistema
• adozione di documentazione tecnica recante tutte le informazioni necessarie alle autorità per valutare la conformità dei sistemi di AI ai requisiti
• conservazione delle registrazioni degli eventi (log)
• trasparenza e fornitura di informazioni e misure di sorveglianza umana
• adeguati livelli di accuratezza, robustezza, cybersicurezza

Sistemi a rischio limitato

Per i sistemi che interagiscono con gli individui, per quelli di riconoscimento delle emozioni e di categorizzazione biometrica (non inclusi tra quelli vietati) nonché per quelli che generano o manipolano contenuti (deepfake) v'è l'**obbligo di informare l'utente che sta interagendo con un sistema di intelligenza artificiale o del fatto che un particolare contenuto è stato creato attraverso l'intelligenza artificiale** (ad esempio, i social Facebook e Instagram di Meta e la piattaforma YouTube di Google sono già in linea), al fine di consentire all'utente di utilizzare la tecnologia in modo informato e consapevole

Regime sanzionatorio

L'AI Act prevede sanzioni molto gravi in caso di mancato rispetto delle disposizioni vigenti

Da 10 a 40 milioni di euro o dal 2% al 7% del fatturato annuo globale dell'azienda, a seconda della gravità della violazione

La presentazione di documentazione falsa o fuorviante alle autorità di regolamentazione è sanzionata severamente