IL NUOVO EU AI ACT

DIRITTI, RESPONSABILITÀ E OPPORTUNITÀ DELL'INTELLIGENZA ARTIFICIALE

14 novembre 2023

Vittorio Tommasone

Counsel IBM Italy & IBM Sustainability Software Europe

AIGI
ASSOCIAZIONE ITALIANA GIURISTI DI IMPRESA

SISTEMI AD ALTO RISCHIO

Rischio valutato facendo riferimento a:

- ✓ **Settori** considerati a rischio
- ✓ **Usi** considerati rischiosi

Definizione **tecnologicamente neutrale** di sistemi di AI

➡ **Foundation models e general purpose AI tool** non considerati high risk systems di per sè, ma soggetti a specifiche previsioni

USI PROIBITI

1. Utilizzo di **tecniche subliminali o di manipolazione** che agiscono senza che una persona ne sia consapevole

2. Utilizzo teso a **sfruttare vulnerabilità** di uno specifico gruppo di persone, dovute all'età o alla disabilità fisica o mentale

3. Utilizzo di sistemi di **classificazione biometrica** (salvo a fine terapeutico e previo specifico consenso informato)

4. Utilizzo per per **valutare affidabilità** delle persone fisiche per un determinato periodo di tempo sulla base del loro comportamento sociale o di caratteristiche personali (*social scoring*) o per valutare **potenziali rischi di condotte criminali** da parte di singoli individui o gruppi di individui tramite profilazione

USI PROIBITI - *Segue*

5. Utilizzo per creare o svilppare **database di facial recognition** raccogliendo immagini da internet o da telecamere di sorveglianza
6. Utilizzo di sistemi per **interpretare le emozioni** degli individui nell'ambito dell'esercizio dei poteri delle forze dell'ordine, immigrazione, educazione o sui luoghi di lavoro
7. uso di sistemi di **identificazione biometrica remota <u>in tempo reale</u>** in spazi accessibili al pubblico
8. uso di sistemi di **identificazione biometrica di registrazioni di spazi accessibili al pubblico** a posteriori, salvo autorizzazione preventiva del giudice e nella misura in cui sia strettamente necessaria per le indagini relative ad alcuni specifici reati

REQUISITI PER I SISTEMI DI IA AD ALTO RISCHIO

OBBLIGHI DEI FORNITORI

i. garantire che i loro sistemi di IA ad alto rischio siano **conformi ai requisiti** disposti dal regolamento e siano sottoposti a procedura di **valutazione di conformità**, adottare misure correttive ove necessario;

ii. Assicurarsi che le **persone incaricate della sorveglianza** di un sistema siano specificatamente **informate** dei rischi connessi all'automazione e alla presenza di bias

iii. informare le **autorità nazionali competenti** in merito alla non conformità e alle eventuali misure correttive adottate e su richiesta delle stesse, forniscono a tale autorità tutte le informazioni e la documentazione necessarie per dimostrare la conformità del sistema di IA

OBBLIGHI DEI FORNITORI - *Segue*

iv. Fornire informazioni sui **dati utilizzati** per addestrare il sistema

v. Redigere la **documentazione tecnica** del sistema di IA e conservare i log di sistema;

vi. Indicare i **propri dati** ed apporre la **marcatura CE** sui loro sistemi di IA ad alto rischio per indicare la conformità al regolamento;

vii. Disporre di un sistema di **gestione della qualità** (design, sviluppo, test, data management, communicazione con le autorità competenti);

iv. Rispettare gli **obblighi di registrazione**.

OBBLIGHI DEGLI UTILIZZATORI

1. Usare sistemi **conformemente alle istruzioni** per l'uso che accompagnano i sistemi.

2. **Sorveglianza** Umana

3. Controllo sui **dati di input**.

4. Monitorare il **funzionamento** del sistema di IA

5. Conservare i **log**

6. Ove i sistemi siano utilizzati per prendere decisioni relative ad individui, **informare gli individui** di tale utilizzo

OBBLIGHI DI TRASPARENZA

- I fornitori garantiscono che i sistemi di IA destinati a interagire con le persone fisiche siano progettati e sviluppati in modo tale che le persone fisiche **siano informate del fatto di stare interagendo con un sistema di IA**, a meno che ciò non risulti evidente dalle circostanze e dal contesto di utilizzo.

- Gli utilizzatori di un sistema di riconoscimento delle emozioni o di un sistema di categorizzazione biometrica informano le persone fisiche che vi sono esposte **in merito al funzionamento del sistema**.

- Gli utilizzatori di un sistema di IA che genera **deep fake** sono tenuti **a rendere noto che il contenuto è stato generato o manipolato artificialmente**.

GOVERNANCE E SANZIONI

A livello nazionale:

- ✓ Istituzione di un'**Autorità Nazionale** competente al fine di garantire l'applicazione del Regolamento

A livello EU:

- ✓ Istituzione di un **AI Office**:
- ✓ Istituzione di una **banca dati dell'UE**, accessibile al pubblico, contenente informazioni identificative di foundation models e dei sistemi AI ad alto rischio
- ✓ Promozione di **codici di condotta** volontari

Sanzioni fino al maggiore tra € 40M e 7% del fatturato mondiale totale annuo della società coinvolta

GRAZIE

Vittorio Tommasone

AIGI
ASSOCIAZIONE ITALIANA GIURISTI DI IMPRESA