

L'INNOVAZIONE NELLA SUPPLY CHAIN

HOTEL CROWNE PLAZA MILAN LINATE, 13 GIUGNO 2024

*L'ARTIFICIAL INTELLIGENCE ACT COME STRUMENTO PER LO SVILUPPO DELLA
INNOVAZIONE E DI TUTELA*

TORRENTEVIGNONE STUDIOLEGALE INTERNAZIONALE
AVV. ALESSANDRA VIGNONE

SITO: WWW.TORRENTEVIGNONE.COM
E-MAIL : AV@TORRENTEVIGNONE.COM

PANORAMICA DELL'ARTIFICIAL INTELLIGENCE ACT

13 marzo 2024

Il Parlamento Europeo ha definitivamente approvato l'AI Act - Finalità dell'AI

Ambito di applicazione dell'AI Act ed eccezioni

- «fornitori» dei sistemi di intelligenza artificiale (sia pubblici che privati) che immettono sul mercato o mettono in servizio sistemi di IA nell'UE, indipendentemente da dove i fornitori stessi siano stabiliti, e a quelli situati in un paese terzo, laddove l'output prodotto dal sistema di IA sia utilizzato in Europa
- Operatori
- Importatori
- Distributori
- fabbricanti e rappresentanti autorizzati

TORRENTE VIGNONE STUDIO LEGALE INTERNAZIONALE

13 giugno 2024

1

PANORAMICA DELL'ARTIFICIAL INTELLIGENCE ACT

PRINCIPIO DEL RISCHIO

l'IA può presentare dei rischi per i diritti, la sicurezza delle persone e delle società

- ❖ **INACCETTABILE:** violano i valori e i principi fondamentali dell'UE, come il rispetto della dignità umana, della democrazia e dello stato di diritto **VIETATI**
- ❖ **ALTO:** possono avere un impatto significativo sui diritti fondamentali o sulla sicurezza delle persone. Questi sistemi sono soggetti a rigorosi obblighi e requisiti prima di poter essere immessi sul mercato o utilizzati **OBBLIGHI /REQUISITI / CONTROLLI**
- ❖ **LIMITATO:** possono influenzare i diritti o le volontà degli utenti, ma in misura minore rispetto ai sistemi ad alto rischio. **OBBLIGHI INFORMATIVI PER UTENTI**
- ❖ **MINIMO:** non hanno alcun impatto diretto sui diritti fondamentali o sulla sicurezza delle persone, offrono ampi margini di scelta e controllo agli utenti **NO OBBLIGHI**

PANORAMICA DELL'ARTIFICIAL INTELLIGENCE ACT LA REGOLAMENTAZIONE DEI MODELLI GPAI (GENERICI E SISTEMICI)

CODES OF PRACTICE PER I MODELLI GPAI: L'AI ACT PREVEDE CHE, IN ATTESA DELLA PUBBLICAZIONE DI STANDARD EUROPEI ARMONIZZATI, ENTRAMBE LE CATEGORIE DI MODELLI GPAI, GENERICI E SISTEMICI, POSSANO BASARSI SU “CODES OF PRACTICE” PER DIMOSTRARE IL RISPETTO DEGLI OBBLIGHI LORO INCOMBENTI (DOCUMENTI TECNICI CHE SPECIFICANO GLI STANDARD DA SEGUIRE)

CONTROLLI ESEGUITI DAL **AI OFFICE** (COMMISSIONE EUROPEA)

TORRENTE VIGNONE STUDIO LEGALE
INTERNAZIONALE

13 giugno 2024

GLI ADEMPIMENTI IN MERITO AI SISTEMI DI AI OBBLIGHI PER SVILUPPATORI/FORNITORI E UTILIZZATORI DI SISTEMI DI IA

GLI OBBLIGHI CAMBIANO A SECONDA DEL TIPO DI RISCHIO

I SISTEMI DI IA AD ALTO RISCHIO

- CONFORMITÀ AI REQUISITI TECNICI
- IDENTIFICAZIONE
- LA DOCUMENTAZIONE TECNICA
- L'INFORMAZIONE AGLI UTENTI
- LA SUPERVISIONE UMANA, LA SICUREZZA E LA PRECISIONE
- **UNA VALUTAZIONE DEL RISCHIO** E A STABILIRE UN SISTEMA DI GESTIONE DELLA QUALITÀ
- OBBLIGHI DI REGISTRAZIONE, TRACCIABILITÀ E SEGNALAZIONE

TORRENTE VIGNONE STUDIO LEGALE INTERNAZIONALE

13 giugno 2024

1

GLI ADEMPIMENTI IN MERITO AI SISTEMI DI IA

I SISTEMI DI IA A RISCHIO LIMITATO

- OBBLIGO DI COMUNICARE AGLI UTENTI CHE STANNO INTERAGENDO CON UN SISTEMA DI IA E DI FORNIRE LORO INFORMAZIONI PERTINENTI SULLE SUE CARATTERISTICHE E LIMITAZIONI. (INFORMAZIONI DEVONO ESSERE CHIARE, COMPENSIBILI E ACCESSIBILI)

I SISTEMI DI IA A RISCHIO MINIMO

- NON SONO SOGGETTI A NESSUN OBBLIGO NORMATIVO
- DEVONO COMUNQUE RISPETTARE LE LEGGI E I REGOLAMENTI GENERALI APPLICABILI ALL'IA, COME IL GDPR, QUELLI RELATIVI ALLA CONCORRENZA, AI DIRITTI DEI CONSUMATORI.

SANZIONI PREVISTE

- AVVERTIMENTI O DIFFIDE DA PARTE DELLE AUTORITÀ NAZIONALI COMPETENTI - MISURE CORRETTIVE (RITIRO/DISABILITAZIONE DEL SISTEMA)
- **FINO A 35 MILIONI DI EURO O AL 7% DEL FATTURATO TOTALE ANNUO** A LIVELLO MONDIALE DELL'ESERCIZIO FINANZIARIO PRECEDENTE (A SECONDA DI QUALE SIA IL VALORE PIÙ ALTO) PER LE VIOLAZIONI RELATIVE ALLE PRATICHE VIETATE O ALLA NON CONFORMITÀ AI REQUISITI SUI DATI;
- **FINO A 15 MILIONI DI EURO O AL 3% DEL FATTURATO TOTALE ANNUO** A LIVELLO MONDIALE DELL'ESERCIZIO FINANZIARIO PRECEDENTE PER LA MANCATA OSSERVANZA DI UNO QUALSIASI DEGLI ALTRI REQUISITI O OBBLIGHI DEL REGOLAMENTO, **INCLUSO MODELLI GPAI**
- **FINO A 7,5 MILIONI DI EURO O ALL'1,5% DEL FATTURATO MONDIALE ANNUO TOTALE** DELL'ESERCIZIO PRECEDENTE PER LA FORNITURA DI INFORMAZIONI INESATTE, INCOMPLETE O FUORVIANTI AGLI ORGANISMI NOTIFICATI E ALLE AUTORITÀ NAZIONALI COMPETENTI IN RISPOSTA A UNA RICHIESTA

LE SANZIONI SONO APPLICATE DALLE AUTORITÀ NAZIONALI COMPETENTI

ENTRATA IN VIGORE DELL'AI

IL REGOLAMENTO SI APPLICHERÀ DUE ANNI DOPO LA SUA ENTRATA IN VIGORE DALLA PUBBLICAZIONE NELLA GAZZETTA UFFICIALE DI UNIONE EUROPEA, CON ALCUNE ECCEZIONI PER DISPOSIZIONI SPECIFICHE:

- | | |
|--------------------------------------------------------------------------------------------|------------|
| ➤ DIVIETI DI PRATICHE VIETATE | 6 MESI |
| ➤ CODICI DI CONDOTTA | 9 MESI |
| ➤ CONTROLLI SUI SISTEMI DI AI PER FINALITÀ GENERALI, COMPRESA LA GOVERNANCE (MODELLI GPAI) | 12 MESI |
| ➤ OBBLIGHI PER I SISTEMI AD ALTO RISCHIO | 24/36 MESI |

GRAZIE PER LA VOSTRA ATTENZIONE

AVV. ALESSANDRA VIGNONE

TORRENTE VIGNONE STUDIO LEGALE INTERNAZIONALE

SITO: WWW.TORRENTEVIGNONE.COM

E-MAIL : AV@TORRENTEVIGNONE.COM

L'INNOVAZIONE NELLA SUPPLY CHAIN

L'ARTIFICIAL INTELLIGENCE ACT COME STRUMENTO PER LO SVILUPPO DELL'INNOVAZIONE E DI TUTELA

MILANO, 13 GIUGNO 2024



TORRENTE VIGNONE
STUDIO LEGALE INTERNAZIONALE

AVV. GRAZIA TORRENTE

LA RACCOLTA DEI DATI PER IL TRAINING

- Per creare strumenti di AI, è necessario un training molto intenso e, quindi porre attenzione alla raccolta di dati, ottenere i migliori possibili per realizzare strumenti efficaci.
- Più alta è la qualità del dato raccolto, più elevata sarà la qualità del risultato.
- La tipologia di dati dovrà essere la più ampia possibile: immagini, testi, video, audio, raccolti attraverso modalità automatizzate o meno.
- Ciò che conta è che si crea un «latent space», i dati vengono letti come vettori numerici, parametri statistici



QUESTIONI LEGALI PER I DATASET PER I MODELLI AI

- Il vero controllo non è sull' «output» del sistema ma è sui dati di partenza: devono essere di alta qualità e in grandi quantità, sempre crescenti.
- Ciò ha portato le aziende a recuperare sempre più dati anche non avendone il diritto di utilizzo.
- OpenAI lo sa bene: ha chiesto al Parlamento inglese di poter godere di una deroga commerciale per il training di ChatGPT! Diceva «*impossibile to create AI tools like ChatGPT without copyrighted material*»



AI ACT

- Come si interviene, quindi, a livello legislativo?
- «Any use of copyrighted content requires permission from the rights holder, unless copyright exceptions and limitations apply»
- I fornitori di servizi di AI generative devono «implement a policy to comply with Union copyright law»
- Quindi: (i) qualsiasi utilizzo di dati per addestramento è valido **solo con il consenso** e (ii) i fornitori di AI devono fornire un sommario di dati utilizzato



VIOLAZIONI AL DIRITTO D'AUTORE E GDPR

- Casi già sanzionati a livello europeo:
- Google condannata dal CNIL con multa di \$270M in Francia in quanto utilizzati dati per Gemini in violazione del GDPR
- In Olanda casi simili in cui il Garante Privacy ha affermato che è illegale la raccolta di dati in Internet senza consenso
- Garante italiano il 29.01.24 contesta OPEN AI - ChatGPT per violazioni GDPR
- Aziende pensavano di poter far affidamento sul fatto che i servizi e tutta la materia fossero nuovi e quindi su una «assenza» di regolamentazione specifica MA ciò non era vero.
- Ora creato a livello europeo l'AI Office per attuare l'AI Act



QUALI SOLUZIONI

- Accordi con giornali o editori importanti per regolamentare l'utilizzo di dati in articoli o testi, o immagini stabilendone un compenso all'autore o possessore del dato.
- Questo il trend di Google e di Open AI
- Altro trend quello dei social
- **ATTENZIONE!** Meta ha stabilito nelle proprie condizioni richieste di autorizzazioni per utilizzare i dati degli utenti per addestrare l'AI.



COME TUTELARSI SE SI È DISEGNATORI/CREATORI DI MACCHINARI?

- Utilizzare software denominati «Nightshade and Glaze» sviluppati dall'Università di Chicago che rendono inutilizzabili i propri lavori se presi per il training o addirittura distruggono l'immagine stessa.
- Veri e propri contratti di licenza con i fornitori di AI Generativa
- Stabilire compensi equi e tutele sulla tipologia di utilizzi



RISCHI SE SI ACQUISTANO SISTEMI DI AI GENERATIVA

- Proprietà intellettuale: rischio di violazione dei diritti di proprietà intellettuale, qualora il dataset di addestramento include contenuti protetti da copyright e licenze
- Mancata protezione dei dati confidenziali riservati e personali immessi in un sistema di AI



TUTELE SE SI ACQUISTANO SISTEMI DI AI GENERATIVA

- Ove possibile, verifiche dei dataset di addestramento a campione, in ogni caso,
- **INCLUDERE NEI CONTRATTI** di servizi clausole di garanzia in cui venga dichiarato che non siano state utilizzate informazioni, immagini, ecc. che fossero coperte dalla legge d'autore e, ove lo fossero, siano state acquisite le autorizzazioni necessarie.
- **ATTUARE LE MISURE PRIVACY** nei **CONTRATTI** chiedendo che tutti i dati immessi, comprese le immagini siano stati acquisiti osservando gli adempimenti privacy del GDPR

