

IL CODICE ETICO PER L'INTELLIGENZA ARTIFICIALE: UN COMMENTO SULLA BOZZA INIZIALE

19 dicembre 2024

AUTORI

Aurora Agostini

Partner



Giulietta Minucci

Counsel



Jessica Giussani

Associate



Giovanni Lombardi

Associate



Con l'adozione del primo Codice di Condotta Generale per l'Intelligenza Artificiale (AI), ci troviamo dinanzi a un momento cruciale per il futuro della regolamentazione di questa tecnologia. Il progetto, promosso ai sensi dell'AI Act (Regolamento UE 2024/1689), rappresenta un ambizioso tentativo di bilanciare innovazione tecnologica, tutela dei diritti fondamentali e sicurezza dei sistemi di intelligenza artificiale.



IL CONTESTO NORMATIVO

Il Codice di Condotta, attualmente in fase di consultazione, si inserisce in un quadro normativo definito dall'AI Act, entrato in vigore il 1° agosto 2024. L'obiettivo principale è quello di guidare i fornitori di modelli di intelligenza artificiale a uso generale verso standard di trasparenza, sicurezza e affidabilità. A tale scopo, il documento si ispira ai principi dell'Unione Europea, come sancito nella Carta dei diritti fondamentali e nei trattati comunitari.

Il documento sottolinea l'importanza di una regolamentazione che tenga conto dei rischi sistemici legati all'uso dei modelli di AI a uso generale, come definiti dall'articolo 3, paragrafo 65 dell'AI Act, con particolare attenzione a quelli caratterizzati da un elevato rischio sistemico secondo i criteri stabiliti dall'articolo 51, paragrafo 1.

La bozza del Codice è organizzata intorno a quattro aree principali:

- **Trasparenza e Regole sul Copyright:** Obblighi di documentazione dettagliata per garantire la tracciabilità dei modelli e il rispetto delle normative sul diritto d'autore.
- **Identificazione e Mitigazione dei Rischi Sistemici:** Strumenti per valutare e gestire i rischi associati a modelli con potenziale sistemico, come la manipolazione su larga scala o l'uso improprio in ambiti critici.
- **Governance dei Rischi:** Meccanismi di supervisione e segnalazione che coinvolgono autorità competenti e altri stakeholder.
- **Proporzionalità:** Differenziazione delle misure basata sulla dimensione del fornitore, con semplificazioni per PMI e startup.



PROFILI DI RESAPONSABILITÀ

Particolare rilevanza assumono le disposizioni inerenti alla responsabilità dei fornitori di modelli di AI a uso generale. Il Codice, in attuazione dell'articolo 53 dell'AI Act, delinea un articolato sistema di obblighi che include:

- la predisposizione e l'aggiornamento continuo della documentazione tecnica del modello, comprensiva del processo di training e testing;
- l'implementazione di politiche di compliance con il diritto dell'Unione in materia di copyright;
- a pubblicazione di un sommario dettagliato sui contenuti utilizzati per l'addestramento del modello.

Per i fornitori di modelli con rischio sistemico, l'articolo 55 introduce ulteriori obblighi sostanziali, tra cui la valutazione e mitigazione dei rischi sistemici a livello dell'Unione, nonché il monitoraggio e la documentazione degli incidenti rilevanti, secondo quanto specificato nel paragrafo 1, lettere a), b) e c) della norma.

MISURE TECNICHE E OPERATIVE

Il Codice introduce, in attuazione dell'articolo 56 dell'AI Act, l'obbligo di adottare un Safety and Security Framework (“**SSF**”), strumento fondamentale per la gestione del rischio e la documentazione delle misure di sicurezza implementate. Tale framework deve includere, secondo quanto previsto dalla Sezione 2 dell'Allegato XIII, dettagliate procedure di valutazione continua e misure di mitigazione calibrate sulla base della severità dei rischi identificati.

Il sistema di monitoraggio e reporting, disciplinato dall'articolo 55, paragrafo 1, lettera c), prevede obblighi specifici di documentazione e segnalazione tempestiva all'AI Office e alle autorità nazionali competenti. Particolare rilevanza assume, in questo contesto, la definizione di incidente grave ai sensi dell'articolo 3, paragrafo 49 dell'AI ACT.

ASPETTI CRITICI E OPPORTUNITÀ

Uno dei punti di maggiore interesse riguarda la definizione e l'applicazione dei criteri di trasparenza: la bozza all'articolo 53 prevede, ad esempio, che i fornitori di AI rendano pubbliche informazioni dettagliate sui dataset utilizzati, i metodi di addestramento e i parametri principali dei modelli. Tuttavia, resta da chiarire come conciliare tali obblighi con la protezione del know-how industriale e dei segreti commerciali.



Un altro aspetto fondamentale è il riconoscimento della necessità di una cooperazione internazionale per lo sviluppo di standard interoperabili, un tema particolarmente rilevante per modelli open-source e tecnologie transnazionali. In merito vale la pena ricordare il regime differenziato previsto dall'articolo 53, paragrafo 2, per i modelli open-source, per i quali alcune disposizioni risultano disapplicate, fermi restando gli obblighi fondamentali in materia di rischi sistemici secondo quanto specificato dai considerando 102 e 103.

La versione definitiva del Codice, attesa per maggio 2025, ed il successo dell'implementazione dipenderà in larga misura dalla capacità di bilanciare le esigenze di flessibilità normativa con la necessità di garantire standard elevati di sicurezza e protezione dei diritti fondamentali, come richiesto dall'articolo 1 dell'AI ACT: in questo contesto, sarà essenziale lo sviluppo di meccanismi efficaci di cooperazione tra le autorità competenti, secondo quanto previsto dall'articolo 74, paragrafo 10, assicurando al contempo un approccio proporzionato che tenga conto delle esigenze specifiche di realtà imprenditoriali anche di piccole e medie dimensioni (PMI e startup innovative).



AUTORI



Aurora Agostini

Partner



Giulietta Minucci

Counsel



Jessica Giussani

Associate



Giovanni Lombardi

Associate



Questo documento è fornito a scopo informativo generale e non intende fornire consulenza legale sui temi trattati. I destinatari di questo documento non possono fare affidamento sui suoi contenuti. LEXIA e/o i professionisti dello studio non possono essere ritenuti responsabili in alcun modo per i contenuti di questo documento, né sulla base di un incarico professionale né per qualsiasi altra ragione.