CAPCO

L'AI NEI SERVIZI FINANZIARI DOPO L'ENTRATA IN VIGORE DEL REGOLAMENTO EUROPEO SULL'INTELLIGENZA ARTIFICIALE (AI ACT)

a wipro company

A novembre 2023, abbiamo pubblicato un articolo sulla governance dell'intelligenza artificiale, dimostrando come una prospettiva basata sui dati, combinata con nuovi ruoli dedicati alla governance e alla conformità dell'AI, possa ridurre significativamente i rischi nell'implementazione delle soluzioni di intelligenza artificiale

Dopo l'adozione dell'AI Act, abbiamo colto l'opportunità di riesaminare il nostro framework di governance per l'intelligenza artificiale in modo da assicurarci che rispetti i nuovi requisiti normativi.

In questo nuovo documento, mostriamo che un approccio rigoroso alla governance dell'AI può fornire un framework di controllo necessario per conformarsi al nuovo Act e rappresentare una checklist per garantire una continua conformità.

Destinato a fornire un framework normativo e legale comune per l'intelligenza artificiale, il Regolamento mira a definire un'AI affidabile, promuovendo un ambiente sicuro e favorevole all'innovazione per utenti, sviluppatori e aziende.

Il Regolamento si applica all'uso dell'AI all'interno dell'UE, indipendentemente dal luogo geografico di appartenenza del fornitore, seguendo un principio simile a quello stabilito per il GDPR, è entrato in vigore 20 giorni dopo la pubblicazione nella Gazzetta ufficiale dell'UE, avvenuta a giugno 2024.

La nuova legge suddivide i tipi di intelligenza artificiale in base al livello di rischio. I sistemi di IA a basso rischio saranno soggetti a minimi obblighi di trasparenza, mentre quelli ad alto rischio dovranno rispettare diversi requisiti per accedere al mercato dell'UE. Saranno vietati i sistemi di IA considerati troppo pericolosi, come la manipolazione cognitiva e il punteggio sociale. Inoltre, la legge proibisce l'uso dell'IA per politiche predittive basate sulla profilazione e per la classificazione delle persone tramite dati biometrici, come razza, religione o orientamento sessuale.

Le regole dell'AI Act prevedono tempistiche di applicabilità scaglionate, lasciando alle aziende il tempo per prendere confidenza con il nuovo Regolamento. In linea generale, il Regolamento sarà applicabile a decorrere dal 2 agosto 2026.

Tuttavia, alcuni requisiti saranno applicabili già dal 2025, in particolare così come previsto dall'Articolo 113 "Entrata in vigore e applicazione":

- I capi I e II (definizioni e pratiche vietate) si applicano a decorrere dal 2 febbraio 2025;
- Il capo III, sezione 4 (autorità di notifica designate dagli stati membri), il capo V (modelli di AI per finalità generali), il capo VII (banca dati UE per i sistemi ad alto rischio), il capo XII (sanzioni) e l'art. 78 (riservatezza dei dati trattati in conformità al regolamento) si applicano a decorrere dal 2 agosto 2025, ad eccezione dell'art. 101 (Sanzioni pecuniarie per i fornitori di modelli di IA per finalità generali);
- L'art. 6, paragrafo 1 (classificazione dei sistemi ad alto rischio), e i corrispondenti obblighi di cui al Regolamento, si applicano a decorrere dal 2 agosto 2027

La Commissione Europea evidenzia i benefici dell'integrazione della regolamentazione come fondamento per lo sviluppo delle applicazioni di intelligenza artificiale. Secondo le varie direttive dei servizi finanziari dell'UE, le autorità competenti sono incaricate di supervisionare e garantire l'applicazione delle normative. Esse devono assicurare la conformità e la sorveglianza del mercato dei sistemi di AI utilizzati dalle istituzioni finanziarie regolamentate, con la facoltà per gli stati membri di delegare questa responsabilità ad altri enti designati.

Le autorità dispongono dei poteri previsti dalle normative vigenti per svolgere attività di sorveglianza e far rispettare la conformità in modo efficace.

I legislatori europei chiariscono che i servizi finanziari sono già sottoposti a regolamentazioni e controlli estremamente rigorosi.

Il Regolamento Europeo sull'AI non introduce nuovi obblighi o modifiche al quadro normativo generale (come DORA, MiFIR/MiFID, EBA GLOM), ma rappresenta una regolamentazione aggiuntiva, supervisionata in maniera simile alle normative esistenti.

AI -categoria di rischio	AI ACT- Tempistiche
Rischio Inaccettabile	Classificati come rischio inaccettabile sono i sistemi di intelligenza artificiale che influenzano significativamente gli utenti tramite tecniche manipolative, ingannevoli o sfruttando le loro vulnerabilità, come i giocattoli vocali che incoraggiano comportamenti pericolosi nei minori. Anche i sistemi di "social scoring" e quelli per la profilazione predittiva di comportamenti illeciti, nonché i sistemi di identificazione biometrica senza adeguate garanzie democratiche. Per via del rischio di violazione dei diritti fondamentali, i seguenti sistemi vengono considerati vietati, salvo eccezioni previste. Le disposizioni previste al capo II inerenti le pratiche vietate saranno applicabili a decorrere dal 2 febbraio 2025
Rischio Alto	Identificati al Capo III nell'AI Act, sono classificati a rischio alto i sistemi che possono influire su salute, sicurezza o diritti fondamentali; esempi di sistemi ad alto rischio includono quelli per l'accesso agli istituti di istruzione, il reclutamento di personale, l'identificazione biometrica remota, la categorizzazione biometrica basata su attributi sensibili e il riconoscimento delle emozioni. Questi sistemi dovranno soddisfare rigorosi requisiti per essere ammessi nell'UE. Gli adempimenti per i sistemi di IA ad alto rischio troveranno applicazione dal 2 agosto 2026, salvo eccezione per i sistemi di IA ad alto rischio che rientrino nell'elenco della normativa di armonizzazione dell'Unione presente all'interno dell'Allegato I.
Rischio Trasparenza	Il Capo IV riguarda i sistemi di IA destinati ad interagire direttamente con le persone fisiche, o che generano o manipolano immagini, contenuti, audio o video e che quindi possono comportare specifici rischi di furti di identità, manipolazioni o inganni (ad esempio, i chatbots o i c.d. deep fake). A tale riguardo, sono previsti specifici obblighi di informazione e trasparenza. In particolare: (i) rendere gli utenti consapevoli del fatto che la loro interazione avviene con una macchina quando si utilizzeranno tali sistemi di intelligenza; (ii) segnalare espressamente i contenuti generati dall'intelligenza artificiale (ad esempio, i deep fake; (iii) nella progettazione di sistemi di IA, il contenuto sintetico di audio, video, testo e immagini dovrà essere contrassegnato in un formato leggibile dalla macchina e riconoscibile come generato o manipolato artificialmente. L'IA in questa categoria di rischio deve conformarsi al regolamento entro il 2 agosto 2026.
Rischio Sistemico per modelli di IA per finalità generali	I modelli di IA per finalità generali con rischio sistemico sono quelli che potrebbero avere un impatto significativo sul mercato interno e sulla società, ad esempio sulla salute pubblica, sicurezza e diritti fondamentali. Oltre ai requisiti di trasparenza e protezione del diritto d'autore, i fornitori di questi modelli devono valutare e mitigare costantemente i rischi, garantendo anche un adeguato livello di cybersicurezza. Le prescrizioni relative ai sistemi di IA per finalità generali riportate al Capo V troveranno applicazione dal 2 agosto 2025.
Rischio Minimo	Si tratta di sistemi con rischi minimi o nulli per i diritti e la sicurezza dei cittadini, come i sistemi di raccomandazione e i filtri antispam. Questi sistemi non avranno obblighi specifici, ma potranno seguire volontariamente codici di buone pratiche. Il regolamento non si applica.

LE PRIORITÀ NELLA GOVERNANCE

Il Regolamento sull'IA dell'UE illustra chiaramente diversi esempi di applicazione della governance all'intelligenza artificiale. Ad esempio, garantisce che i sistemi di AI siano costruiti in modo conforme, che i dati di addestramento siano di alta qualità tecnica e non sollevino preoccupazioni etiche, sociali o ambientali. Inoltre, l'output dei sistemi di AI deve essere spiegabile, tracciabile e rispettare le questioni di proprietà intellettuale, mentre gli utenti che interagiscono con l'AI devono esserne sempre consapevoli.

La governance prevede anche un monitoraggio costante di tutti questi aspetti e, in caso di violazioni o scenari imprevisti, i soggetti che impiegano tali tecnologie devono segnalare immediatamente tali eventi alle autorità competenti.

La Commissione Europea enfatizza costantemente l'importanza di diversi principi chiave nello sviluppo e nell'uso dell'intelligenza artificiale: privacy, trasparenza, diversità, non discriminazione, equità, e benessere sociale e ambientale. Questi standard impongono il rispetto delle leggi sulla privacy vigenti, garantiscono l'uso trasparente dell'AI, evitano impatti discriminatori e tengono conto delle conseguenze sociali e ambientali.

Questi principi servono da linee guida durante la progettazione e l'utilizzo dei modelli di AI. Inoltre, il Regolamento stabilisce che "i dataset di addestramento, validazione e test di alta qualità richiedono l'implementazione di pratiche appropriate di governance e gestione dei dati. Questi dataset devono essere sufficientemente rilevanti, rappresentativi, privi di errori e completi rispetto allo scopo previsto del sistema."

Infine, il Parlamento Europeo ha evidenziato specifiche preoccupazioni riguardo all'Intelligenza Artificiale Generativa (GenAI) nei requisiti per il Regolamento sull'IA. La GenAI, che include modelli di linguaggio di grandi dimensioni (LLM), si sta rapidamente diffondendo, portando a potenziali abusi dei dataset e sollevando preoccupazioni sulla proprietà intellettuale. Esiste infatti il rischio di violazione del copyright attraverso output generati dalla GenAI o tramite tecnologie deep fake. Quest'ultime rappresentano una minaccia significativa, creando intenzionalmente contenuti ingannevoli che contribuiscono alla disinformazione e fuorviano il pubblico. Il Parlamento Europeo ha sottolineato la necessità di governance in questo contesto durante la fase di consultazione del regolamento.

CAPCO: MODELLO DI GOVERNANCE DELL'AI

Il nostro modello di governance dell'Intelligenza artificiale rappresenta un buon punto di partenza pratico per le istituzioni di servizi finanziari che iniziano il loro percorso di conformità.

I tre risultati chiave che qualsiasi tipo di governance dell'AI deve fornire per conformarsi al Regolamento Europeo sono i seguenti:

- **Spiegabilità dei risultati dell'AI** : la spiegabilità offre trasparenza, consente il rilevamento e la mitigazione dei bias, supporta l'identificazione e la correzione degli errori e stabilisce la proprietà dei diritti di proprietà intellettuale nei contenuti generati dall'AI
- **Protezione della proprietà intellettuale e dei dati sensibili** (inclusa la protezione della riservatezza delle informazioni sensibili e la conformità con altre normative, ad esempio il GDPR)
- **Contrasto alle allucinazioni.**

La nostra soluzione si può articolare in tre sotto-soluzioni, ciascuna correlata direttamente ai tre risultati chiave. L'elemento fondamentale è l'automazione, che richiede un approccio concettuale e permette l'adozione di procedure standardizzate, ripetibili e imparziali per garantire che i risultati siano misurabili e comparabili.

L'automazione può essere applicata con successo in relazione ai tre risultati chiave della governance dell'AI, nello specifico:

- Creare un tracciamento tra gli output dell'AI e le informazioni in input attraverso l'uso di metadati e informazioni contestuali.
- Proteggere la proprietà intellettuale mediante l'automazione end-to-end nel trattamento delle informazioni.
- Contrastare le allucinazioni integrando conoscenze esterne, aumentando i dati disponibili e utilizzando il prompting intelligente. In questo contesto, l'automazione si ottiene sfruttando tecnologie disponibili come la generazione aumentata dal recupero (RAG) o fornendo semantica aggiuntiva tramite la creazione e l'implementazione di grafi di conoscenza/knowledge.

La figura seguente fornisce una panoramica ad alto livello del nostro modello di governance dell'IA (descrizioni dettagliate dei processi coinvolti possono essere trovate nel nostro documento originale).

Sebbene l'automazione da sola non possa risolvere tutte le sfide associate a un modello di governance dell'intelligenza artificiale, essa avrà un impatto cruciale nella riduzione delle attività ripetitive e di routine, liberando così risorse che potranno essere destinate a compiti più complessi.

		CICLO DI VITA DELLE INFORMAZIONI E DELLA CONOSCENZA						
		01 Pre-elaborazione	02 Elaborazione					03 Post-elaborazione
OVERVIEW SOLUZIONE - ACCELERATORE GOVERNANCE		Le informazioni grezze in ingresso vengono etichettate / annotate	Le Pipeline CI/ CD relative alla conoscenza elaborano automaticamente gli input	Database Grafo (che riflette il dominio della conoscenza)	Export del Database in formato di testo strutturato	Script Python che trasforma l'export in Linguaggio Naturale	Training Personalizzato ("Fine Tuning") O API per Ingegneria del Prompt	I guardrail vengono applicati a Gen-AI
GOVERNANCE	RISULTATI	Essere in grado di spiegare i risultati forniti dall'IA	Protezione della proprietà intellettuale e delle informazioni sensibili					Lotta contro le allucinazioni
	CONTROLLO	[a1] Esiste una traccia documentata tra l'input (informazioni fornite all'IA) e il risultato restituito dall'IA.	[b3] Il modello Gen-AI e la pipeline di elaborazione delle informazioni vengono distribuiti in un ambiente con accesso limitato.			[b2] Le tecniche di anonimizzazione e oscuramento dei dati vengono impiegate per rimuovere qualsiasi informazione identificativa dai dati di input.		[c1] I guardrail vengono applicati ai modelli per impedire che forniscano informazioni al di fuori di determinati confini.

Soluzione di automazione della governance dell'IA overview[1]

RUOLI E PARTECIPAZIONE ESECUTIVA

Un altro elemento fondamentale per il successo dell'implementazione dell'AI è l'introduzione di nuovi ruoli e membri nel progetto. Poiché i requisiti normativi influenzano lo sviluppo e l'uso dell'AI in generale, e di quella generativa in particolare, sarà necessario istituire nuovi ruoli per garantire la conformità alle normative. Questo aspetto è particolarmente rilevante nel settore dei servizi finanziari.

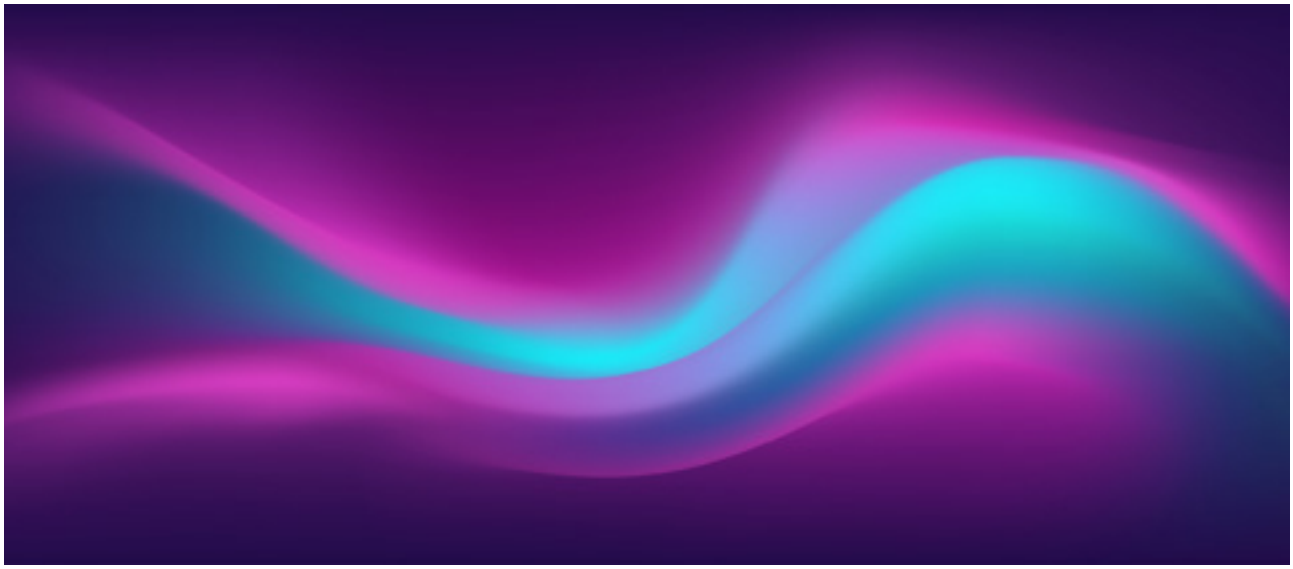
La necessità di integrare i compiti di governance nei progetti del ciclo di vita dello sviluppo software (SDLC) è in costante aumento, soprattutto con l'emergere della GenAI e delle nuove normative sull'AI.

I nuovi ruoli essenziali per supportare questi processi includono:

- **Responsabile della Governance dell'AI**: Sovrintende l'implementazione e l'esecuzione dei modelli di governance dell'IA, inclusi monitoraggio continuo, qualità del tracciamento e reportistica.
- **Manager del Rischio AI**: Identifica e valuta i rischi associati all'IA, quantificandoli, mitigandoli, tracciandoli e riportandoli.
- **Responsabile della Conformità dell'AI**: Garantisce la conformità alle leggi e normative pertinenti, inclusi gli obblighi di reportistica verso le autorità (inserimento dei sistemi di AI e dei loro metadati nei database dell'UE e segnalazione degli incidenti).
- **Responsabile dell'Etica dell'AI**: Assicura l'uso etico dell'AI, monitorando l'utilizzo di dati etici e sostenibili e garantendo output etici.
- **Architetto Tecnico dell'AI**: Progetta e implementa l'infrastruttura tecnica a supporto del modello di governance dell'AI.

Sebbene alcuni di questi ruoli si sovrappongano, richiedono competenze e organizzazioni di progetto molto diverse, non tutte ancora comunemente conosciute o considerate best practice.

Capco ha sviluppato un approccio pratico per integrare questi ruoli all'interno delle organizzazioni finanziarie. Con l'aumento costante dell'implementazione e dello sviluppo dell'AI e delle applicazioni correlate, questi ruoli e responsabilità possono evolvere. In sostanza, il personale e le responsabilità possono sovrapporsi e una singola persona o unità che può coprire più ruoli. Tuttavia, le responsabilità fondamentali derivanti dal framework di governance dovranno comunque essere affrontate.



CONCLUSIONE

Con il rapido sviluppo dell'AI, è prevedibile che anche le normative evolvano di pari passo. L'articolo 73 del Regolamento sull'AI dell'UE conferisce alla Commissione Europea il potere di modificare aspetti chiave del Regolamento, inclusa la definizione di sistemi di AI ad alto rischio, i requisiti di documentazione tecnica, la valutazione della conformità e la dichiarazione di conformità dell'UE.

La gestione continua della qualità e del rischio da parte dei fornitori di prodotti o servizi che incorporano l'AI è essenziale per i rilasci post-mercato, al fine di mantenere la fiducia e la conformità. Sebbene attualmente la maggior parte dei sistemi di AI nelle istituzioni finanziarie sia considerata a basso rischio, le aziende devono essere consapevoli che gli sviluppi futuri potrebbero alterare questa classificazione.

I nuovi ruoli di governance, così come i dipartimenti di Compliance esistenti, possono essere supportati nei loro sforzi di conformità dall'intelligenza artificiale stessa. Ad esempio, le tecniche di GenAI possono essere utilizzate per monitorare e analizzare le pubblicazioni degli organi di regolamentazione, evidenziando quali parti delle normative nuove o aggiornate diventano applicabili. Inoltre, i responsabili delle applicazioni, dei processi o dei prodotti pertinenti possono essere allertati, e quindi le misure di conformità possono essere identificate e pianificate di conseguenza.

Migliorando la struttura del loro sistema di conformità per garantire un framework robusto di governance, le istituzioni finanziarie possono essere sicure e adeguarsi agli impatti dei futuri cambiamenti normativi.

COME PUÒ AIUTARE CAPCO

L'approccio di Capco, che prevede l'implementazione di nuovi ruoli di governance e l'aumento del grado di automazione, risponde alle sfide normative del nuovo Regolamento Europeo sull'Intelligenza Artificiale ed è allineato alla sua lungimirante impostazione.

Il nostro framework assicura la conformità ai requisiti delle normative esistenti, come MaRisk, BAIT, DORA e MiFID, che non sono ancora state sostituite dal Regolamento AI.

Integrando una struttura di governance adeguata alla configurazione dei vostri progetti di AI o GenAI, sarete pronti per le future iniziative normative.

Contattateci per scoprire come Capco può supportarvi in questo processo, dalla definizione di un framework di governance dell'IA e nuovi ruoli di governance, fino al monitoraggio automatizzato e all'implementazione dei cambiamenti normativi.

5. REFERENCES

1. https://www.capco.com/Capco-Institute/Journal-58-Artificial-Intelligence/Applied-Generative-AI-Governance
2. https://artificialintelligenceact.eu/
3. TA (europa.eu)
4. https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/757583/EPRS_BRI(2023)757583_EN.pdf
5. Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity by Claudio Novelli, Federico Casolari, Philipp Hacker, Giorgio Spedicato, Luciano Floridi :: SSRN
6. Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale)Testo rilevante ai fini del SEE. (europa.eu)

AUTORI

Peter Lehnen, Consulente Principale
Igor Schnakenburg, Direttore Principale
Gerhardt Scriven, Direttore Esecutivo
Alessandro Corsi, Partner

CONTATTI

Paolo La Torre, paolo.latorre@capco.com
Luca Iaccarino, luca.laccarino@capco.com
Teresa Vozza, teresa.vozza@capco.com

CAPCO

Capco è una società di Wipro che opera a livello globale nella consulenza tecnologica e direzionale specializzata nel guidare la trasformazione dei settori dell'energia e dei servizi finanziari. Capco agisce all'intersezione tra business e tecnologia combinando pensiero innovativo con una conoscenza del settore senza pari per accelerare le iniziative digitali nei settori del banking e dei pagamenti, dei mercati dei capitali, della gestione patrimoniale e degli asset, delle assicurazioni e dell'energia. La capacità innovativa di Capco prende vita attraverso la sua cultura premiata Be Yourself At Work e attraverso il suo talento diversificato.

Per saperne di più, visita www.capco.com o seguici su LinkedIn, Instagram, Facebook e YouTube.

UFFICI NEL MONDO

APAC
Bengaluru – Electronic City
Bengaluru – Sarjapur Road
Bangkok
Chennai
Gurugram
Hong Kong
Hyderabad
Kuala Lumpur
Mumbai
Pune
Singapore

MEDIO ORIENTE
Dubai

EUROPA
Berlino
Bratislava
Bruxelles
Dusseldorf
Edimburgo
Francoforte
Ginevra
Glasgow
Londra
Milano
Parigi
Vienna
Varsavia
Zurigo

NORD AMERICA
Charlotte
Chicago
Dallas
Hartford
Houston
New York
Orlando
Toronto

SUD AMERICA
São Paulo

WWW.CAPCO.COM

CAPCO
a wipro company

JN_6023