Un approccio alla Governance dell'AI

Governance è una parola complicata e un po' fumosa, perché essa include tutti i processi di governo aziendali. È il modo in cui le regole o le azioni sono strutturate, mantenute e regolamentate compreso il modo in cui viene assegnata la responsabilità. Garantire la *governance* dell'IA implica che l'IA sia spiegabile, trasparente ed etica. Queste tre parole significano cose diverse per organizzazioni diverse o funzioni all'interno delle stesse. Ad esempio, esiste una differenza tra una definizione tecnica e una definizione politica (o legale) di "trasparenza".

Una politica di *governance* deve esistere, essere comunicata e interagire con il mondo che la circonda e all'interno dell'organizzazione. La *governance* dell'IA deve adattarsi al quadro generale della *governance* aziendale e, a volte, potrebbe essere necessario essere incentrata sulle macchine e non essere ottimizzata per gli esseri umani.

In generale, la *governance* IA include **tutti i processi di *governance:*** il modo in cui le regole o le azioni sono strutturate, mantenute e regolamentate e come sia attribuita la relativa responsabilità.

Possiamo riassumere tre fattori che sintetizzano gli aspetti di governance:

- Misure: la capacità di misurare costi, valore, verificabilità e conformità;
- Software e Dati: i dettagli sul codice software e sui singoli componenti dei dati;
- Quadro aziendale: la necessità di adattarsi al quadro generale di governo dell'organizzazione.

La chiave è che, per tutte le organizzazioni, la definizione

della *governance* dell'IA deve essere fatta con accuratezza e riflessione garantendo che la responsabilità sia trasparente e misurabile.

Di chi è a carico la **responsabilità** della *governance* dell'AI?

La domanda è complicata, perché oggi non esiste una sola persona unicamente responsabile e la risposta varierà in base alla definizione di *governance* dell'IA fatta da un'organizzazione. È opportuno che ogni responsabile sia informato sull'IA in tutte le funzioni aziendali, nel coinvolgimento dei clienti, nei prodotti e nella *supply chain*. La *governance* dell'IA deve essere pertinente e applicabile a tutti i leader di un'organizzazione, compresi anche ruoli funzionali e operativi di un'organizzazione.

Il CEO deve essere la persona responsabile della Carta della *governance* dell'IA (lo sponsor), nonché della chiara assegnazione di responsabilità all'interno dell'organizzazione e delle misure necessarie per il controllo.

I diversi ruoli funzionali all'interno di un'organizzazione devono essere inclusi nella *governance* dell'IA: ad esempio Il *General Counsel*, il CFO, il *Chief Data Officer* (CDO), il DPO.

Assegnare la responsabilità della *governance* dell'IA è essenziale. Senza chiare responsabilità, nessuno è responsabile.

Risulta quindi fondamentale definire correttamente i **ruoli** all'interno dell'organizzazione, così come porre delle misure sulla *governance* dell'AI.

La mancanza di misure risulterà allora un punto debole in qualsiasi organizzazione, anche perché non possono essere trasferite e incorporate in processi, sistemi e piattaforme (mancanza di controllo).

Quali misure allora sono rilevanti e di chi ne è la

responsabilità? Alcune misure o metriche per la *governance* dell'IA diventeranno e dovranno diventare degli standard per le organizzazioni attraverso regole o procedure.

Di seguito alcuni dei KPI che le organizzazioni dovrebbero considerare:

- Dati: misurare la tipologia, la discendenza, la provenienza e la qualità dei dati.
- Sicurezza: dei dati, dei modelli e sul loro utilizzo. Consentire la comprensione della manomissione o dell'uso improprio degli ambienti IA.
- Costo / valore: misurare il costo dei dati o anche il valore creato dai dati e dall'algoritmo.
- *Bias*: sono richiesti KPI che possono mostrare *bias* di selezione o di misurazione, monitorandoli continuamente attraverso dati diretti o derivati.
- Responsabilità: chiarezza di responsabilità, ruoli e coinvolgimento degli individui.
- *Audit*: raccolta continua di dati, che in forma aggregata potrebbero costituire la base per audit e revisioni periodiche del
- Tempo: le misure del tempo consentono una migliore comprensione dell'impatto nel tempo.

La *governance* dell'IA dovrebbe far parte di tutti gli ambienti di intelligenza artificiale e *machine learning*, con un approccio olistico permeato in tutta l'organizzazione.

Possiamo porci quattro domande di sintesi:

1) La IA è trasparente?

Come affermato in precedenza, se l'organizzazione dispone di IA, deve esserlo etica, spiegabile e trasparente. Ricordiamo che c'è una differenza tra trasparenza giuridica e tecnica. Se non si è in grado di rispondere a questa domanda, è il momento di riesaminare il software.

2) Chi è responsabile?

Attenzione: la responsabilità non ricade nelle mani di un unico ruolo, ma anche a ruoli funzionali come membri del consiglio di amministrazione, amministratori delegati, CFO, CDO e consulenti legali; ricorda di incorporarli nella *governance* dell'IA della tua organizzazione.

3) Quali misure chiave dovresti considerare?

Ci sono diverse misurazioni che bisogna considerare quando si misura la *governance* dell'IA all'interno dell'organizzazione, il tutto a seconda di come questa viene definita.

4) Hai messo in atto un framework di analisi?

Se la risposta a questa domanda è no, è opportuno considerare l'installazione un robusto framework che misuri automaticamente – o anche manualmente – la *governance* dell'IA relativa ai modelli e ai dati.

Per rispondere all'ultima domanda possiamo utilizzare il framework sviluppato e indicato nel precedente articolo *Modello di autovalutazione relativo a un sistema di Intelligenza Artificiale,* che illustra come attraverso una metodologia che si ispira al CSF NIST (attraverso le funzioni, categorie e sottocategorie) sia possibile effettuare un'autovalutazione relativamente ai 7 principi dell'AI:

1. supervisione umana;
2. robustezza e sicurezza;
3. privacy, controllo e gestione dei dati;
4. trasparenza;
5. diversità, correttezza, assenza di discriminazione;
6. benessere sociale e ambientale;
7. responsabilità.

Concludendo, come tutti i processi che impattano sull'organizzazione aziendale, sugli utenti e sui clienti,

anche la AI necessità di un processo di *governance* generale che – attraverso un approccio olistico – possa garantire la piena comprensione e coscienza delle attività implementate e dell'impatto delle stesse.

Articolo a cura di **Stefano Gorla**

Stefano Gorla è nato a Milano, si è laureato in fisica nucleare presso l'Università di Padova. Ha insegnato per qualche anno Matematica e Fisica presso alcuni licei.

Da anni si occupa di privacy e sicurezza dei dati attraverso un approccio sistemico e olistico.
Consulente e formatore in ambito sicurezza e tutela dei dati e delle informazioni e relatore in numerosi convegni.

Auditor ISO 27001, DPO Certificato FAC Certifica, NIST Specialist Certificato Fac Certifica, Certificato COBIT5 ISACA, Master EQFM.
Ha maturato notevoli esperienze come Referente Privacy (DPO) e consulente in tali ambiti.
È autore di varie pubblicazioni sul tema.

https://www.ictsecuritymagazine.com/articoli/un-approccio-alla-governance-della-ai/