Università
Ca'Foscari
Venezia

Università Ca' Foscari Venezia
Dorsoduro 3246, 30123 Venezia
P.IVA 00816350276 - CF 80007720271
www.unive.it

Linee guida per l'impiego di strumenti di IA ai fini del miglioramento dei servizi amministrativi

Premesse

L'intelligenza artificiale, spesso abbreviata in "IA" (o "AI" in inglese), raggruppa diverse tecnologie che eseguono compiti o si comportano in modo "intelligente". Secondo l'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE), l'intelligenza artificiale va intesa come un sistema che, per determinati obiettivi definiti dall'uomo, può effettuare previsioni, dare raccomandazioni o prendere decisioni con diversi livelli di autonomia.
Negli ultimi anni ci sono stati sviluppi importanti nell'ambito della cosiddetta "AI generativa" ("GenAI") creando grandi aspettative sugli impieghi degli strumenti di questo tipo per una grande varietà di scopi, inclusa la creazione di diverse forme di contenuti (testi, immagini, audio, video, codice, dati, ecc.) sulla base di istruzioni (prompt) fornite dall'utente.
D'altra parte non è ancora del tutto chiaro come gli strumenti di IA possano essere sfruttati al meglio, eppure è innegabile che le recenti evoluzioni in questo campo creino molte nuove opportunità per supportare e automatizzare almeno parzialmente i processi delle Pubbliche Amministrazioni.
Il principale vantaggio derivante dall'uso di questi strumenti sarà probabilmente la possibilità di aumentare la produttività, specialmente per attività o processi ripetitivi che richiedono molto tempo, e necessitano di un apporto intellettuale limitato
Inoltre, questi strumenti possono contribuire a migliorare la qualità del lavoro, ad esempio gli strumenti di IA possono aiutare il personale delle pubbliche amministrazioni ad analizzare i dati, a migliorare i testi prodotti e a renderli disponibili in lingue differenti dall'italiano attraverso delle traduzioni automatiche.
Queste linee guida intendono sviluppare una visione strategica sugli strumenti di IA e fornire maggiore chiarezza su ciò che l'Ateneo considera un uso appropriato o meno di tali strumenti nei processi amministrativi, sostenendone e incoraggiandone l'impiego da parte del personale dell'Ateneo e al contempo segnalandone i limiti e i rischi potenziali.
L'Università Ca' Foscari Venezia si impegna, dunque, a orientare, promuovere e supportare l'uso responsabile dell'IA generativa nelle attività di ricerca, a monitorare l'utilizzo di strumenti di IA all'interno della propria organizzazione, nonché a diffondere i principi etici, le buone pratiche e le opportune tutele a garanzia della sicurezza, della privacy e del copyright.

Ambito di applicazione delle linee guida

Queste linee guida si riferiscono all'uso di strumenti di IA generativa nei processi in carico al Personale Tecnico Amministrativo, concentrandosi principalmente su quelli disponibili a livello commerciale/pubblico, indipendentemente dal loro campo di applicazione (ampio o specifico) e dal tipo di input/output (es. testo, immagini o dati). Le linee guida si applicano anche agli strumenti di IA disponibili in determinati programmi tramite plug-in, sia online che offline.
Non si applicano, invece, ai processi per l'uso o lo sviluppo di strumenti di IA come parte integrante delle attività scientifiche e di didattica per cui sono in definizione linee guida specifiche.

Principi generali

L'Ateneo è aperto all'uso di strumenti di IA per migliorare le attività amministrative e per agevolare la sperimentazione pone poche restrizioni specifiche. Ad esempio, anche se gli strumenti di IA sono resi disponibili tramite licenze open source, è necessario tener conto della legislazione vigente nazionale e internazionale e in particolare dell'AI Act dell'Unione europea: questo vieta l'IA che rappresenta una minaccia per l'uomo (es. IA con rischi inaccettabili). Inoltre devono essere rispettate la legislazione e le norme applicabili in termini di sicurezza, salute, benessere e tutela dei diritti umani.
L'impiego di strumenti di IA a fini nell'ambito del miglioramento dei servizi amministrativi dovrebbe sempre rispettare i seguenti principi generali, in linea con i valori chiave di affidabilità, onestà, rispetto e responsabilità indicati nelle Linee guida sull'uso responsabile dell'IA generativa nella ricerca a cura della Commissione europea:

- il personale tecnico amministrativo resta pienamente responsabili dei risultati dell'IA nonché dell'adeguatezza dei processi amministrativi in cui l'intelligenza artificiale viene utilizzata. La responsabilità non può essere trasferita agli strumenti di IA e il PTA ha la responsabilità di tenersi sempre aggiornato sulle loro modalità di utilizzo. Ciò comporta che il PTA è responsabile per l'eventuale uso inappropriato di questi tool, per esempio per il mancato rispetto delle norme sul copyright (plagio, citazione di fonti, ecc.). Gli autori restano infatti pienamente responsabili del contenuto dei loro scritti, anche delle parti prodotte da uno strumento di IA, e sono quindi colpevoli di qualsiasi violazione dell'etica di pubblicazione.
- il PTA deve verificare i risultati degli strumenti di IA, adottando vari passaggi di controllo. Si dovrebbero sempre cercare le fonti originali e, ove applicabile, controllare le licenze dell'opera originale.
- Il PTA deve essere consapevole che l'uso degli strumenti di IA può anche rappresentare uno svantaggio in alcune circostanze. Ad esempio gli strumenti di IA possono generare testo con dichiarazioni generiche o del tutto inventato e quindi non legato a dati reali.
- Occorre tenere in considerazione che malgrado i contratti di licenza qualunque dato offerto come input a sistemi di AI verrà trattato da sistemi informatici che spesso non

risiedono all'interno della comunità Europea e che potrebbero determinare un trattamento problematico ai fini della privacy.

Il PTA è dunque tenuto a non inserire negli strumenti di IA i seguenti dati:

- dati personali, che possono portare direttamente o indirettamente all'identificazione di persone;
- dati importanti in vista di una futura valorizzazione della ricerca o che sono (o possono essere) protetti dalla normativa sulla proprietà intellettuale;
- dati il cui rilascio potrebbe essere eticamente problematico, ad esempio per rischio di uso inappropriato o danno di gruppo, come in caso di stigmatizzazione;
- dati soggetti a contratti con terze parti (es. aziende);
- dati protetti da copyright o da vincoli di riservatezza, salvo che con l'autorizzazione del proprietario;
- in linea generale è consigliato per il PTA di accertarsi che le impostazioni sulla privacy degli strumenti di IA impiegati siano corrette e di modificarle laddove necessario.

Vantaggi dell'uso dell'IA nelle attività amministrative

L'intelligenza artificiale (IA) si presenta come un nuovo valido strumento di cui l'Ateneo può avvalersi in particolare per velocizzare e potenziare le attività quotidiane e i processi standardizzabili, in particolare quelli in cui sono coinvolte attività complesse ma ripetitive. Tra i vantaggi che si possono individuare dall'uso di questi strumenti troviamo:

- aumentare la produttività. I compiti più onerosi in termini di tempo, ripetitivi o che non richiedono contributi intellettuali sostanziali da parte del personale tecnico amministrativo possono essere almeno parzialmente demandati agli strumenti di IA. Inoltre tali strumenti possono anche rafforzare le competenze del PTA permettendo ad esempio l'analisi di grandi moli di dati o la sintesi di lunghi documenti.
- per determinate competenze, ridurre il divario di conoscenza tra il PTA. I soggetti meno qualificati potrebbero trarre maggiori benefici dall'uso degli strumenti di IA rispetto ai soggetti più qualificati: ad esempio un impiegato non molto esperto nella gestione di una particolare attività potrebbe utilizzare uno strumento di IA per compensare questa carenza per individuare il corretto procedimento amministrativo ed essere supportato nella stesura degli atti.
- gli strumenti di AI potrebbero permettere la revisione di regolamenti e di circolari permettendo di verificare quelli di nuova introduzione con particolare riguardo alla loro compatibilità con le linee guida, le circolari e i regolamenti già presenti oltre che con le norme in essere.
- gli strumenti di IA possono essere utilizzati per riassumere e spiegare testi e regolamenti, avvicinandosi maggiormente al pubblico e aiutando a spiegare in modo più facilmente comprensibile i processi amministrativi.

Limiti e potenziali problemi nell'uso degli strumenti di IA per la ricerca

Come descritto in precedenza, l'utilizzo degli strumenti di IA può avere evidenti vantaggi. Tuttavia, occorre essere consapevoli che tali strumenti possono anche presentare alcune gravi carenze, sia per limiti tecnici dei tool che per un loro non corretto utilizzo. Altri rischi potrebbero derivare dalla natura proprietaria di alcuni strumenti o dalla concentrazione della loro proprietà su singole aziende.
Di seguito sono esposti i principali rischi a cui fare attenzione ed alcune buone prassi da mettere in atto per evitarli. Non si tratta di una lista esaustiva: è raccomandabile sviluppare una capacità critica con l'uso e la pratica.

Rischio: informazioni sbagliate, allucinazioni, elaborazioni errate.
A volte l'IA può fornire dei risultati errati, a volte solamente imperfetti, altre volte completamente inventati, senza alcun riscontro con la realtà. Spesso questi risultati vengono esposti in maniera del tutto convincente e argomentati con riferimenti, citazioni ed esempi che, per quanto credibili, sono in realtà inesistenti.
Buone prassi: In caso di elaborazione di dati, estrazioni, analisi ecc. fare sempre dei controlli, almeno a campione, sulla correttezza dei risultati. Per fare questo è importante non chiedere solamente il risultato di un'elaborazione, ma anche come poterla replicare. E' opportuno poi richiedere anche eventuali riferimenti a siti, libri o articoli su cui è basato il ragionamento in modo da poterne verificare la validità e verificare che gli stessi libri o articoli citati esistano realmente

Rischio: divulgazione / pubblicazione di dati e informazioni segrete, personali o riservate. Generazione di informazioni sensibili (giuste o sbagliate).
Sebbene i gestori della maggior parte dei sistemi di IA dichiarino che le informazioni sottoposte ad analisi non vengano "assimilate" per usi futuri, data la complessità di questa tecnologia non si può ancora garantire al 100% che questo non accada. Inoltre, una delle principali capacità dell'IA è proprio quella di cercare correlazioni e generare nuovi dati a partire da quelli a disposizione, per questo esiste il rischio che vengano generate informazioni sensibili sugli utenti senza che queste siano state effettivamente fornite. Tale informazioni potrebbero poi essere divulgate involontariamente ad esempio in risposta a richieste di altri utenti.
Buone prassi: non sottoporre mai informazioni personali, riservate, segrete o sensibili ai sistemi di IA. Se è necessario utilizzare o analizzare queste informazioni, bisogna prima trattarle opportunamente e anonimizzarle ad esempio togliendo identificativi chiave come matricole, codici fiscali, indirizzi ecc.. Tali riferimenti possono essere sostituiti da chiavi anonime, ad esempio sostituendo la matricola con il semplice numero di riga in excel, così sarà poi possibile riconciliare il risultato con il dato reale.
Attenzione: se si forniscono troppe informazioni (es sesso, età, indirizzo, corso di laurea ecc..) l'IA potrà generare un profilo delle persone incrociando i dati. Un'altra buona prassi sarà, ad

esempio, quella di sostituire i comuni di nascita o residenza con indicazioni generiche del tipo "comune 1", "comune 2" ecc... e mantenere a parte una tabella di corrispondenze. Si potranno fare comunque analisi del tipo "qual è il comune da cui provengono la maggior parte degli studenti" salvo poi tradurre esternamente il risultato (es "comune 23" = "Venezia") con quello reale. Per maggiore sicurezza sarebbe bene cambiare questa corrispondenza ad ogni nuova analisi o quando si sottopongono nuovi dati.

Rischio: pregiudizi, discriminazione.
L'IA è stata istruita con le informazioni presenti nel web, nei libri, nelle riviste ecc.. Quanto più alta e affidabile è la qualità delle informazioni utilizzate tanto più lo saranno i risultati generati. Una fonte dati perfetta però non esiste: spesso ci sono insidie, fake news, notizie manipolate e queste possono alterare il funzionamento degli algoritmi portandoli a fornire risultati che, sebbene corretti e documentati, sono incompleti o tendenziosi perché minati da pregiudizi. Come per gli essere umani, anche per l'IA l'obiettività del giudizio è un elemento di criticità
Buone prassi: una buona prassi può essere quella di usare e confrontare più sistemi in modo da avere più punti di vista (spesso anche l'operatore può essere vittima degli stessi pregiudizi dello strumento) oppure far valutare a uno strumento il risultato di un altro. In ogni caso i pregiudizi dipendono anche dai dati forniti e da come vengono sottoposte le domande, quindi il migliore controllo rimane quello dell'operatore che deve sviluppare una certa sensibilità sull'argomento.

Rischio: violare il diritto d'autore, essere accusati di plagio, generare documenti non originali.
L'IA può essere utilizzata anche per generare immagini, testi, relazioni, documenti, composizioni musicali, poesie, sceneggiature, idee commerciali ecc. Teoricamente quanto viene generato è un prodotto originale. L'IA però viene istruita utilizzando informazioni preesistenti quindi c'è il rischio che il risultato sia molto simile, se non uguale, a qualcosa di già esistente e potrebbe violare il diritto d'autore o essere accusabile di plagio.
Buone prassi: se quanto generato deve essere divulgato, pubblicato, venduto ecc. è opportuno fare una ricerca approfondita sia sui riferimenti forniti dall'IA stessa (si può chiedere se quanto generato è ispirato a qualcosa di preesistente) sia esternamente con altri strumenti per cercare di capire cosa è originale e cosa non lo è e comportarsi di conseguenza (es. con crediti, riferimenti bibliografici, citazioni ecc.). Infine è buona prassi segnalare cosa è stato generato con l'IA in modo che gli utilizzatori siano consapevoli di eventuali rischi.

Rischio: perdita di controllo e dipendenza dall'uso dell'IA.
Anche supponendo che le problematiche finora esposte non esistano, l'uso indiscriminato di questi strumenti rischia di portare alla perdita di controllo sui processi decisionali e sugli strumenti adottati. Ad esempio se si generano delle formule excel per automatizzare calcoli senza capirle, o del codice di programmazione, o si chiedono delle elaborazioni di dati e si usa il risultato senza capire come è stato calcolato, nel tempo si rischia di cedere il controllo delle informazioni all'IA e, in caso di problemi, di non essere più in grado di ricostruire i processi decisionali adottati.

Buone prassi: quando si chiede una elaborazione, la generazione di formule o il calcolo di un risultato chiedere sempre anche che vengano spiegati i passaggi con cui il dato è stato fornito e cercare di capire il ragionamento e verificare di poterlo replicare autonomamente. Questo permette di mantenere un approccio critico, in cui si delega all'IA l'onere di una operazione ripetitiva, ma non la conoscenza e la competenza per la gestione del dato o dell'informazione. Solo in questo modo l'IA diventa uno strumento per la crescita e la formazione personale e non un assistente che fa, privo di controlli, il lavoro al posto nostro.

Rischio: dati non aggiornati.
I dati di addestramento per gli strumenti di IA potrebbero essere datati. Gli strumenti di IA, inclusi i LLM, potrebbero non avere accesso agli eventi o alle pubblicazioni più recenti (per esempio il limite di conoscenza di GPT-3.5 era settembre 2021 perché le fonti successive a quella data non erano incluse nei dati di addestramento).
Buone prassi: In caso di stesura di testi fare sempre dei controlli, almeno a campione, sulla correttezza di quanto riportato e sull'aggiornamento del dato. Per fare questo è importante non chiedere solamente il risultato di un'elaborazione, ma eventuali riferimenti a siti, libri o articoli su cui è basato il testo da poterne verificare la validità e verificare che gli stessi libri o articoli citati esistano realmente e siano aggiornati.

Usi vietati dalla normativa

La comunità europea ha approvato una legge che regolamenta l'uso dell'Intelligenza artificiale, il Regolamento (UE) 2024/1689 (detta IA Act) che vieta alcune applicazioni specifiche di questa tecnologia. Sebbene siano regolamentati degli aspetti molto specifici raramente utilizzati nelle attività di un normale ufficio è comunque bene tenere a mente quali siano:

- Creazione indiscriminata di banche dati di informazioni biometriche estrapolate da internet o videosorveglianza.
- Riconoscimento automatico delle emozioni al lavoro o a scuola.
- Profilazione e azioni di polizia predittiva.
- Valutazione / categorizzazione automatica dei cittadini (cd "punteggio sociale").
- Sistemi di manipolazione del comportamento umano.

C'è da ricordare infine che anche il GDPR, all'articolo 22, stabilisce che i cittadini hanno diritto a non essere sottoposti a decisioni basate unicamente su processi automatizzati, questo implica che se ad esempio una graduatoria, un'ammissione, una esclusione ecc.. è stata stabilita automaticamente da un software o un algoritmo, l'interessato ha diritto a contestare la decisione e chiedere spiegazioni o una rivalutazione da un essere umano. Per tale motivo in questi casi è importante avere sempre il controllo su come avvengono questi processi in modo da poterli esporre e replicare.