POLITECNICO
MILANO 1863

DIPARTIMENTO DI
ARCHITETTURA E
STUDI URBANI

Raccomandazioni sull'utilizzo responsabile di strumenti di intelligenza artificiale di natura generativa

L'adozione di strumenti di intelligenza artificiale (IA) generativa quali ad esempio Microsoft Copilot, ChatGPT, Gemini, Midjourney comporta specifici rischi per la protezione dei dati personali a causa della configurazione dei sistemi e delle modalità di interazione con gli utenti.

Questi sistemi, basati su tecnologie di apprendimento profondo ed elaborazione del linguaggio naturale, possono elaborare e generare dati sensibili che, se non gestiti correttamente, possono causare danni.

Il Politecnico di Milano opera in un contesto pubblico che richiede stretta conformità alle normative esistenti. L'uso di IA per scopi di interesse pubblico necessita di una valutazione approfondita per dimostrarne la necessità, la proporzionalità e l'allineamento con gli obiettivi istituzionali.

Principali rischi per la protezione dei dati personali associati a sistemi di IA generativa:

- Re-identificazione
- Elaborazione involontaria di dati personali
- Registrazione e conservazione dei dati
- Generazione e deduzione di output sensibili
- Personalizzazione e profilazione
- Accesso e uso da parte di terzi
- Mancanza di trasparenza
- Perdita del controllo dei dati
- Uso dei dati per decisioni automatizzate

Criticità da considerare nell’ambito della privacy:

- **Archiviazione e gestione dei dati**: assicurarsi che i risultati delle elaborazioni siano archiviati in modo sicuro dallo strumento IA.
- **Eliminazione dei dati**: Gli utenti devono poter eliminare la cronologia delle interazioni per mantenere un certo grado di controllo personale sui dati archiviati.

- **Sede dei dati**: verificare nelle condizioni contrattuali dove sono collocati i server utilizzati dallo strumento AI. Solo i server collocati nell'UE garantiscono il rispetto del Regolamento UE2016/679**.**
- **Utilizzo dell'IA sul Web**: restrizioni allo strumento IA per contenuti locali (escludendo il Web) sono fondamentali per mantenere l'integrità e la confidenzialità delle informazioni gestite. Disabilitare l'accesso al Web garantisce questa confidenzialità ed evita potenziali fughe di dati. Quando si utilizza l'IA sul Web, le risposte ottenute devono essere gestite senza compromettere la sicurezza dei dati interni o esporre l'Ateneo a rischi di privacy e/o di violazione del diritto d'autore.
- **Estendibilità**: prestare attenzione all'uso di plug-in e connettori aggiuntivi poiché possono introdurre rischi per la protezione dei dati personali. L'uso di questi strumenti crea un collegamento tra l'IA e sistemi esterni, con il possibile transito dei dati in contesti non controllati. Solo i dati necessari devono essere trasmessi, evitando informazioni superflue o sensibili. La definizione dei controlli di accesso deve limitare l'esposizione dei dati solo a chi ne ha bisogno per il tempo necessario.
- **Conformità e normativa**: utilizzare strumenti IA sviluppati da aziende che aderiscono al Regolamento UE 2016/679 e standard di privacy come ISO/IEC 27018. Essere consapevoli delle evoluzioni normative che potrebbero influenzare la gestione dei dati in futuro.

È sconsigliato fornire a sistemi di IA ospitati al di fuori dell'Ateneo dati come:

- Password e nomi utente;
- Informazioni di identificazione personale;
- Dati non anonimizzati;
- Dati protetti da diritto d'autore;
- Dati relativi alla proprietà intellettuale dell'Ateneo;
- Qualsiasi dato che potrebbe danneggiare la reputazione del Politecnico di Milano.

La responsabilità di configurare le interazioni e gestire correttamente i dati personali ricade principalmente sull'utente, con particolare attenzione all'uso di plug-in esterni e alla trasparenza nel trattamento dei dati.

L'uso di plug-in e connettori esterni presenta rischi significativi per la protezione dei dati personali. Pertanto, è fortemente sconsigliato impiegare tali strumenti senza la certezza che rispettino gli standard di privacy e sicurezza imposti dalle terze parti coinvolte.

Qualora l'utente decida di utilizzare plug-in esterni, deve essere consapevole della responsabilità individuale specifica, specialmente se l'uso non è conforme ai requisiti legali e di sicurezza, comportando rischi per la tutela dei dati.