Commenti presentati nell'ambito della consultazione pubblica sulle Linee Guida AGiD per l'adozione dell'IA nella Pubblica Amministrazione

25/03/2025

I seguenti commenti sono il risultato delle riflessioni dell'Osservatorio AI4PA e anche delle considerazioni emerse nel corso del webinar del 14 marzo 2025 «Linee Guida in consultazione e prime applicazioni dell'AI Act Europeo» che ha coinvolto oltre 600 rappresentanti di istituzioni locali e regionali».

Queste osservazioni sono state presentate nell'ambito della consultazione pubblica sulle Linee Guida e riguardano aspetti come la responsabilità legale, la trasparenza, la governance, la formazione delle competenze e la sicurezza, con particolare attenzione alle esigenze delle amministrazioni locali e regionali. La suddivisione per argomenti segue quella proposta da AGiD nella sezione dedicata alle Linee Guida su Forum Italia.

Ambito di applicazione

- Integrare nelle linee guida indicazioni su casi d'uso concreti e sperimentazioni pratiche per supportare le amministrazioni locali nell'applicazione dell'IA ai servizi pubblici.
- Riconoscere formalmente il ruolo delle Province come centrali di committenza per gli acquisti di sistemi di AI nei comuni medio-piccoli e per il relativo sostegno all'implementazione degli stessi. Le linee guida potrebbero specificare le modalità di coinvolgimento delle Province in questo processo.

Riferimenti e sigle

- Esplicitare meglio la questione della responsabilità legale in caso di conseguenze negative dell'IA. Attualmente, la sezione 4.6 (Governance) fa solo un riferimento generico e non chiarisce come affrontare le eventuali responsabilità delle PA nell'utilizzo di sistemi IA. Considerando che l'EU AI Liability Directive è stata ritirata, è necessario precisare quali normative vigenti regolano la responsabilità delle amministrazioni pubbliche nell'uso di IA e quali strumenti possono essere adottati per gestire i rischi legali.

L'Intelligenza Artificiale

- Rivedere il principio di trasparenza nella sezione 3.4 e la correlata sezione 7.2, per evitare che venga interpretato come un divieto per l'utilizzo di IA generativa e reti neurali. Attualmente, l'obbligo di trasparenza assoluta rischia di escludere sistemi avanzati, come quelli basati su reti neurali, che non sono completamente spiegabili ma che possono comunque fornire valore nella PA.

- Considerare l'integrazione di XAI (Explainable AI) come principio guida, consentendo l'uso di sistemi che garantiscano una spiegabilità adeguata, piuttosto che imporre un requisito di trasparenza assoluta che limiterebbe l'adozione di tecnologie IA più avanzate. Sarebbe utile un approccio che equilibri trasparenza ed efficacia, utilizzando la trasparenza come criterio di scelta tra più sistemi disponibili piuttosto che come principio assoluto di adozione.

Modello di adozione dell'IA

- Integrare un riferimento all'uso di sandbox regolatori, ossia ambienti di sperimentazione controllata, per testare soluzioni IA prima della loro adozione su larga scala.
- Definire un'architettura modulare per l'IA nella PA, per consentire alle amministrazioni di adottare strumenti scalabili e adattabili ai diversi contesti locali.
- Modificare la formulazione alla fine di pagina 40, che afferma che i cittadini devono comprendere le decisioni automatizzate. Questo punto è ridondante, poiché il divieto di decisioni automatizzate con impatto significativo sulla vita degli individui è già sancito dall'AI Act e dall'articolo 22 del GDPR. Inoltre, il successivo riferimento al diritto all'intervento umano appare superfluo, in quanto il GDPR già garantisce tale diritto. Sarebbe utile riformulare questa sezione per evitare ripetizioni e allinearla meglio con il quadro normativo vigente.

Conformità delle soluzioni di IA

- Chiarire la definizione del principio di robustezza nella sezione 11, specificando se si intende la capacità di un sistema di fornire risultati coerenti a parità di input oppure la resistenza ai guasti e alle variazioni del sistema.
- Allineare la definizione di robustezza con il significato tecnico comune, distinguendola chiaramente dalla resilienza. Nella terminologia anglosassone, "robustness" indica la coerenza dei risultati a parità di input, mentre nelle linee guida sembra riferirsi alla capacità di funzionare nonostante guasti o variazioni. Questa differenza concettuale potrebbe creare ambiguità nell'interpretazione del principio. Se l'intenzione è riferirsi alla capacità del sistema di mantenere operatività anche in presenza di guasti, allora il termine corretto potrebbe essere resilienza anziché robustezza.

Governance etica dell'IA

- Favorire la creazione di linee guida per una governance condivisa dell'IA nelle amministrazioni locali, evitando duplicazioni e garantendo interoperabilità.

Comunicazione

- Fornire strumenti per ridurre l'asimmetria informativa, in modo che le amministrazioni locali possano adottare l'IA con consapevolezza e non dipendere esclusivamente dai fornitori privati (shopping tecnologico).

Formazione e sviluppo delle competenze

- Esplicitare nelle linee guida la necessità di piani di formazione strutturati per il personale delle PA, per ridurre il divario di competenze nell'uso delle tecnologie IA. Attualmente, la mancanza di competenze è uno degli ostacoli principali all'adozione dell'IA.

ISCRITTA ALL'ANAGRAFE NAZIONALE DELLE RICERCHE DEL MIUR
ACCREDITATA SNA PER LA FORMAZIONE OIV
Viale G. Luporini 37/57 | 55100 Lucca
Tel. +39 0583 582783 | 583342 Fax +39 0583 1900211
info@promopa.it | promopa.it
N°80 Registro Persone Giuridiche Prefettura di Lucca | CF / PI 01922510464

Gestione e qualità dei dati

- Integrare nelle linee guida indicazioni per sviluppare un'architettura modulare e scalabile per la gestione dei dati, favorendo l'interoperabilità tra amministrazioni.

Protezione dei dati personali

- Rivedere il riferimento alle decisioni automatizzate alla fine di pagina 40, in quanto il GDPR già vieta le decisioni automatizzate che impattano significativamente sulla vita dei cittadini.

Sicurezza cibernetica

- Includere indicazioni sulle implicazioni di sicurezza dell'adozione dell'IA, in particolare nelle fasi di sperimentazione e regolamentazione.