

Roma, 8 maggio 2025

Memoria scritta di Microsoft Italia sul Disegno di Legge recante “Disposizioni e deleghe al Governo in materia di intelligenza artificiale” (AC 2316), Commissioni riunite X Attività produttive e IX Trasporti della Camera dei deputati.

Il disegno di legge recante “Disposizioni e deleghe al Governo in materia di intelligenza artificiale” si pone come strumento utile per tradurre, a livello nazionale, il quadro di regole delineato dal Regolamento UE 2024/1689 (“AI Act”), colmando gli spazi di discrezionalità che quest’ultimo affida agli Stati membri e assicurando un’applicazione omogenea e priva di oneri aggiuntivi per imprese e pubbliche amministrazioni. In tale prospettiva, il disegno di legge si reputa debba mirare ad assumere un ruolo strategico di complementarità rispetto all’AI Act europeo, contribuendo a garantirne una piena ed efficace attuazione a livello nazionale. In questo modo si assicurerebbe un equilibrio tra sviluppo dell’intelligenza artificiale e rispetto dei principi fondamentali dell’ordinamento, favorendo al contempo la competitività del sistema produttivo nazionale nonché ad incentivare gli investimenti nel settore, favorendo la crescita di un ecosistema dell’innovazione tecnologica dell’intelligenza artificiale competitivo e all’avanguardia.

In tal senso, appare opportuno richiamare che l’AI Act, così come altre normative dell’UE quali il Regolamento UE 2016/679 (“GDPR”), fornisce un insieme completo ed equilibrato di regole e requisiti per i sistemi di intelligenza artificiale. È pertanto coerente non imporre obblighi aggiuntivi o divergenti che potrebbero frammentare il mercato interno e minare la competitività e il potenziale innovativo del settore europeo dell’intelligenza artificiale. Per tale motivo, si reputa opportuno assicurare la massima coerenza e conformità delle norme nazionali con quelle europee, sia per quanto riguarda i principi espressi a livello europeo in materia di diritto d’autore e privacy, sia evitando l’introduzione di ulteriori obblighi rispetto a quelli già previsti dall’AI Act, in conformità a quanto definito dall’articolo 3, comma 5 del presente disegno di legge. Ciò al fine di evitare possibili ricadute negative nell’adozione, diffusione e sviluppo di questa tecnologia che potrebbero frenare l’innovazione e la competitività delle imprese italiane e della Pubblica Amministrazione e, al contempo, l’attrattività dell’Italia per gli investimenti. Tale impostazione, oltre a garantire la piena aderenza ai principi europei, valorizza anche l’ecosistema italiano: promuove sinergie tra università, centri di ricerca, PMI e start-up, anche attraverso poli di trasferimento tecnologico e sandbox regolatorie, rendendo l’Italia un hub per soluzioni AI affidabili e avanzate.

Con riferimento ad alcuni punti specifici, si esprime apprezzamento per le modifiche introdotte all’articolo 5, lettera d) del disegno di legge con l’esame in Senato. La riformulazione della disposizione rispetto al testo originariamente presentato garantisce ora un equilibrato bilanciamento fra indirizzo pubblico e apertura al mercato. La nuova formulazione evita restrizioni discriminatorie nell’accesso ai servizi di intelligenza artificiale, con la possibilità e non già l’indicazione di privilegiare, nei casi strettamente necessari, la localizzazione e l’elaborazione dei soli dati strategici in data center sul territorio nazionale, senza precludere l’uso delle migliori tecnologie disponibili.

Permangono tuttavia alcuni profili del disegno di legge, in particolare l’articolo 6, che a nostro avviso richiedono ulteriori precisazioni sul piano della coerenza sistemica e della formulazione normativa. Le osservazioni che seguono si concentrano su tali aspetti, nella convinzione che un intervento mirato possa rafforzare ulteriormente l’impianto del provvedimento e la sua efficacia attuativa.

Osservazioni sull'articolo 6 (Disposizioni in materia di sicurezza e difesa nazionale).

L'articolo 6 stabilisce che le attività connesse all'uso di sistemi e modelli di intelligenza artificiale, se condotte per scopi di sicurezza nazionale, cybersicurezza e difesa nazionale, siano escluse dall'ambito di applicazione della normativa prevista dal disegno di legge, e - nella sua attuale formulazione - prevede altresì che i sistemi di intelligenza artificiale destinati al c.d. "ambito pubblico" debbano essere ospitati su server ubicati in Italia, con l'unica eccezione prevista per i sistemi utilizzati all'estero in operazioni di carattere militare.

Si evidenzia, pertanto, la criticità derivante dall'introduzione, in prima lettura al Senato, dell'articolo 6, comma 2, che impone un obbligo generalizzato di localizzazione dei dati in ambito pubblico sul territorio nazionale, in contrasto con l'approccio equilibrato e conforme ai principi di libera circolazione sanciti dalla normativa europea e recepiti all'articolo 5 del presente disegno di legge, oltre che per l'indeterminatezza e l'ambiguità della disposizione, destinata ad applicarsi in via generale ai dati sensibili trattati in ambito pubblico.

- **Possibili ambiguità interpretative**

La formulazione di tale norma presenta alcune ambiguità interpretative, soprattutto in relazione alla definizione di "uso in ambito pubblico". Tale espressione sembrerebbe riferirsi esclusivamente ai sistemi impiegati dalle amministrazioni pubbliche nel contesto della sicurezza e della difesa nazionale, come suggerisce la denominazione dell'articolo, ma potrebbe dare anche adito a interpretazioni più estensive comprendendo anche quelli gestiti da enti privati che forniscono servizi di pubblica utilità o, in alternativa, i sistemi accessibili al pubblico in generale. Un altro elemento di ambiguità e vaghezza è fornito dal riferimento ai "dati sensibili", categoria molto ampia e che si discosta dall'approccio dei "dati strategici" utilizzato nello stesso disegno di legge in esame all'art. 5.

- **Potenziali incompatibilità con il quadro normativo europeo e lo stesso disegno di legge sull'intelligenza artificiale**

Si osserva che l'obbligo di localizzazione previsto dall'art. 6, comma 2, potrebbe entrare in conflitto con il GDPR, che non impone restrizioni geografiche sulla conservazione dei dati, purché siano adottate misure adeguate di protezione. Infatti, il GDPR, oltre a normare i dati trattati in Europa, "si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione" e indica le garanzie ritenute adeguate al trasferimento dei dati e le norme vincolanti da rispettare. È importante quindi sottolineare che anche se le società fornitrici di servizi informatici e di archiviazione si trovano in un territorio extra europeo sono tenute a rispettare il Regolamento europeo. Inoltre, l'AI Act ha stabilito un quadro giuridico dell'Unione che istituisca regole armonizzate in materia di IA per promuovere lo sviluppo, l'uso e l'adozione dell'IA nel mercato interno, garantendo allo stesso tempo un elevato livello di protezione degli interessi pubblici, non prevedendo obblighi specifici di localizzazione dei server, per non compromettere l'integrità del mercato unico digitale. La formulazione della disposizione appare suscettibile di coordinamento con l'articolo 5, comma 1, lett. d), del provvedimento in esame, il quale, in luogo dell'obbligo di localizzazione dei "server" in territorio nazionale, pone in capo allo Stato e alle altre autorità pubbliche competenti il compito di indirizzare le piattaforme di e-procurement delle pubbliche amministrazioni a scegliere fornitori di sistemi e modelli di IA che garantiscono una localizzazione e elaborazione dei dati critici presso "data center" sul territorio nazionale.

L'articolo 6, invece, ad oggi impone un vincolo generalizzato senza considerare la sensibilità dei dati trattati. Si raccomanda, pertanto, l'opportunità di limitare l'obbligo di localizzazione ai dati critici per la difesa e sicurezza nazionale, ai fini di una maggiore chiarezza, di una regolamentazione proporzionata, e mantenendo l'accesso ai dati all'interno del mercato unico digitale.

- **Implicazioni operative e di mercato**

Un'interpretazione estensiva dell'articolo 6, comma 2, potrebbe limitare la concorrenza, restringendo le opzioni a disposizione delle amministrazioni pubbliche nella scelta dei fornitori di soluzioni di intelligenza artificiale. Infatti, l'introduzione di un obbligo di localizzazione dei sistemi di intelligenza artificiale in Italia, comporterebbe una serie di implicazioni operative e di mercato che potrebbero altresì rallentare l'adozione di tecnologie avanzate di intelligenza artificiale e ostacolare il processo di digitalizzazione del settore pubblico, con effetti negativi sulle opportunità di innovazione e sull'adozione di soluzioni avanzate e personalizzate da parte delle amministrazioni pubbliche italiane.

Conclusioni

Alla luce delle criticità illustrate, e come sottolineato anche nel [dossier](#) allegato al provvedimento come trasmesso alla Camera, si auspica una revisione dell'articolo 6, attraverso una revisione testuale – o, in subordine, mediante un'interpretazione autentica – che limiti l'ambito di applicazione della norma ai settori della sicurezza e difesa nazionale, come definiti al comma 1 dello stesso articolo 6, e fornisca coerenza normativa rispetto ai dati di riferimento, potenzialmente includendo la definizione di dati strategici, anziché dati sensibili. Un intervento mirato in tal senso consentirebbe di:

- salvaguardare gli obiettivi di sovranità e sicurezza, senza introdurre vincoli generalizzati che rischiano di confliggere con il quadro giuridico europeo sulla libera circolazione dei dati e con l'approccio "risk-based" accolto all'articolo 5;
- preservare la competitività del settore pubblico e privato, evitandone l'esclusione da soluzioni tecnologiche d'avanguardia e prevenendo oneri sproporzionati per imprese e amministrazioni;
- garantire neutralità tecnologica e concorrenza aperta, elementi essenziali per accelerare la trasformazione digitale della PA.

Difatti, pur perseguendo obiettivi di sicurezza nazionale e sovranità digitale, scopo pienamente condivisibile, tale norma – come attualmente formulata – potrebbe altrimenti comportare rischi significativi per la competitività del settore pubblico e privato, limitando la concorrenza, rallentando l'adozione di tecnologie avanzate e generando difficoltà per le amministrazioni pubbliche e le aziende.

Un equilibrio tra sovranità digitale e apertura al mercato globale risulterebbe cruciale per favorire un'adozione responsabile, sicura e sostenibile delle tecnologie di intelligenza artificiale in Italia.