Anitec-Assinform

Audizione informale presso le Commissioni riunite

IX (Trasporti, poste e telecomunicazioni) e X (Attività produttive, commercio e turismo) della Camera dei deputati

Disegno di Legge

Disposizioni e deleghe al Governo in materia di intelligenza artificiale

(C. 2316 Governo, approvato dal Senato)

A cura di Anitec-Assinform

Associazione Italiana per l'Information and Communication Technology (ICT)
Milano, Via San Maurilio 21, 20123
Telefono 02 0063281
segreteria@anitec-assinform.it – anitec-assinform@pec.it – www.anitec-assinform.it
P.IVA: 10053550967 C.F.: 10053550967

Anitec-Assinform

INTRODUZIONE

Con il Disegno di Legge "Disposizioni e deleghe al Governo in materia di intelligenza artificiale" il Governo ha inteso introdurre una disciplina di livello nazionale su una materia già disciplinata a livello europeo con il Regolamento (UE) 2024/1689 (AI Act), la cui fase di applicazione è già iniziata e si protrarrà nei prossimi anni, con l'obiettivo di regolare specificità nazionali.

In questo contesto, Anitec-Assinform ha evidenziato l'esigenza di assicurare la massima coerenza e conformità delle norme nazionali con quelle europee, sia per quanto riguarda i principi espressi dal Regolamento citato, sia evitando l'introduzione di ulteriori obblighi rispetto a quelli già previsti dall'AI Act. In questo senso, registriamo positivamente come questo principio si rifletta nell'articolo **3, comma 5** del Ddl che è stato aggiunto durante l'esame del provvedimento al Senato.

Introdurre in Italia una disciplina in materia di intelligenza artificiale più restrittiva, o comunque non allineata con quella europea porterebbe a ricadute negative per l'adozione, diffusione e sviluppo di questa tecnologia nelle imprese e nella Pubblica Amministrazione, che potrebbero frenare l'innovazione e la competitività delle imprese italiane e anche l'attrattività dell'Italia per gli investimenti delle imprese straniere.

In linea con questo approccio, oltre all'introduzione del menzionato comma 5 all'**articolo 3**, l'esame al Senato ha introdotto altre modifiche migliorative, quali l'eliminazione della precedente disposizione sul *watermarking* (ex art. 23), una razionalizzazione dei criteri di preferenza per la PA nell'articolo 5, lettera d), e una più chiara disciplina nell'**articolo 8** per l'uso dei dati sanitari per ricerca e sperimentazione tramite IA.

Infine, è opportuno esprimere apprezzamento per la formulazione dell'articolo 25 in materia di diritto d'autore. Il testo approvato raggiunge un buon equilibrio tra i diversi interessi coinvolti e conferma l'aderenza della disciplina nazionale a quella europea (Direttiva Copyright e AI Act).

Ciononostante, **il testo licenziato dal Senato presenta ancora rilevanti profili di criticità** su cui intervenire per chiarire la portata delle norme e garantire certezza giuridica al mercato.

La principale preoccupazione riguarda l'**articolo 6, comma 2**[1], relativo all'obbligo di localizzazione nazionale dei server per l'uso pubblico dell'IA. Tale

[1] TIM non condivide la posizione espressa.

disposizione, pur mossa da finalità di tutela della sicurezza nazionale, introduce un requisito non previsto dall'AI Act, potenzialmente in contrasto con i principi di libera circolazione nel mercato unico e con lo stesso **articolo 3, comma 5** del disegno di legge, nonché in contraddizione con la richiamata **lettera d), comma 1, dell'art. 5 del DDL**. Un'interpretazione estensiva della disposizione, che si riferisce a qualunque tipo di "uso in ambito pubblico" dell'IA, oltre che generare incertezze relative all'applicazione della norma, infatti, rischia anche di limitare fortemente la PA nel suo processo di sviluppo tecnologico, impedendo l'utilizzo e l'accesso alla maggior parte dei modelli e sistemi di IA, alcuni dei quali, peraltro, già adottati da molte amministrazioni pubbliche.

Permangono, inoltre, dubbi interpretativi sul contenuto dell'**articolo 4**, in particolare sull'impatto che la disciplina del consenso per i minori (comma 4) potrebbe avere sui fornitori di sistemi IA, onerandoli, potenzialmente della raccolta del consenso genitoriale in modalità non sempre tecnicamente agevoli o proporzionate al rischio effettivo del sistema utilizzato dal minore. Inoltre, nel contesto più ampio del trattamento dei dati personali per lo sviluppo e l'addestramento di sistemi di IA, si ritiene fondamentale ribadire la validità, accanto al consenso, della base giuridica del **legittimo interesse** ai sensi dell'art. 6 par. 1 lett. f) del GDPR, laddove ne sussistano i presupposti e sia effettuato il necessario bilanciamento con i diritti degli interessati, per non ostacolare l'innovazione.

A ciò si aggiunge l'intervento operato all'**articolo 16**, la cui delega al Governo su dati e algoritmi per l'addestramento appare problematica in quanto un nuovo intervento del Governo potrebbe essere foriero di incertezza per le imprese che, su questi temi, si confrontano con un complesso quadro normativo europeo (GDPR, Data Act, DGA, AI Act), progressivamente in via di applicazione.

Si ritiene, poi, opportuno formulare una considerazione di metodo. La rapida evoluzione dell'intelligenza artificiale impone processi normativi **tempestivi** il cui esito siano norme **chiare e proporzionate**. Solo così è possibile fornire all'ecosistema industriale e dell'innovazione un quadro certo, che non ne imbrigli il potenziale ma ne guidi lo sviluppo in modo efficace. Senza questi elementi l'efficacia delle disposizioni sarebbe ridotta.

In conclusione, si auspica che, nel caso in cui siano approvate modifiche al testo in questa seconda lettura parlamentare, l'esame delle Commissioni competenti

possa focalizzarsi sulla risoluzione delle criticità e delle incoerenze interne al testo ancora presenti e sul pieno allineamento con la disciplina europea in corso di attuazione. Ciò preservando, al contempo, i punti di equilibrio raggiunti in prima lettura su due punti nevralgici del disegno di legge: **l'articolo 5** e, in particolare, **l'articolo 25**. Un tale approccio contribuirebbe, così, a definire un quadro normativo nazionale stabile, chiaro e proporzionato.

OSSERVAZIONI PUNTUALI

Art. 3 (Principi generali)

L'**articolo 3** enuncia i principi generali che governano la ricerca, lo sviluppo e l'applicazione dei sistemi IA in Italia, tra cui il rispetto dei diritti fondamentali, la trasparenza, la proporzionalità, la sicurezza, la protezione dei dati, la non discriminazione, la sostenibilità, l'autonomia umana, la cybersicurezza e l'accessibilità. Il comma 5, aggiunto al Senato, specifica che la legge non introduce obblighi ulteriori rispetto a quelli previsti dall'AI Act.

Osservazioni

Il **comma 5 dell'articolo 3**, che impedisce l'introduzione di obblighi aggiuntivi nell'ordinamento nazionale rispetto al Regolamento (UE) 2024/1689 (AI Act), è fondamentale per garantire la certezza del diritto ed evitare la frammentazione del mercato unico, assicurando che la normativa italiana sia allineata al quadro europeo. **In definitiva, è molto positivo che durante l'esame in Senato sia stat aaggiunta tale disposizione**.

Il comma 5, infatti, garantisce:

- l'aderenza del DDL IA **all'ambito di applicazione** definito dall'AI Act. L'articolo 2 del Regolamento UE esclude esplicitamente dal suo campo di applicazione determinati sistemi ed attività. Di conseguenza il comma 5 dell'articolo 3 del DDL assicura che non siano gravati da obblighi nazionali i sistemi sviluppati o messi in servizio unicamente a fini di ricerca e sviluppo scientifico (art. 2.6 dell'AI Act) e le attività di ricerca, sperimentazione e sviluppo *precedenti* all'immissione sul mercato o messa in servizio (art. 2.8 dell'AI Act), salvaguardando un ambito fondamentale per l'innovazione da vincoli potenzialmente prematuri o inappropriati.
- L'allineamento **all'approccio basato sul rischio** dell'AI Act, **impedendo classificazioni di rischio o requisiti nazionali più stringenti di quelli europei.** L'articolo 6.3 dell'AI Act, ad esempio, chiarisce che anche sistemi elencati nell'Allegato III (relativo a casi d'uso potenzialmente ad alto rischio) *non* sono considerati ad alto rischio se non pongono un rischio significativo di danno alla salute, sicurezza o diritti fondamentali *e* soddisfano specifiche condizioni, quali lo svolgimento di compiti procedurali ristretti o meramente preparatori a una valutazione

rilevante. Per questo, il principio sancito all'articolo 3, comma 5, del DDL è essenziale per assicurare che anche in Italia tali sistemi, pur operando in settori delicati (es. sanità - **art. 7**, giustizia - **art. 15**, lavoro - **art. 11**, professioni intellettuali - **art. 13**), non siano automaticamente soggetti agli oneri dei sistemi ad alto rischio se soddisfano le precise condizioni di deroga previste dall'AI Act.

- La coerenza delle **modalità richieste per assicurare la conformità** dei sistemi IA (ad esempio in materia di sistemi di gestione dei rischi, documentazione tecnica, test, trasparenza, sorveglianza umana) con la disciplina dettagliata negli articoli 8 - 27 dell'AI Act.

L'effettiva portata di tale comma dipende, tuttavia, dalla sua **coerente applicazione** all'interno delle disposizioni del disegno di legge. Come evidenziato nell'introduzione, permangono criticità su alcuni articoli (in particolare l'**art. 6, comma 2**[2], e l'**art. 16**) che sembrano contraddirne lo spirito e la lettera.

Art. 4 (Principi in materia di informazione e di dati personali)

L'**articolo 4, comma 4** regola l'accesso dei minori, richiedendo il consenso genitoriale per i minori di 14 anni e consentendo il consenso diretto dai 14 anni in su, previa adeguata informativa.

Osservazioni

Il comma 4 dell'art. 4 solleva alcune criticità operative.

In primo luogo, si ritiene importante, con riferimento generale al trattamento di dati personali nello sviluppo e addestramento di IA (richiamato implicitamente al comma 2), sottolineare che né la normativa europea, né quella nazionale precludono o obbligano all'utilizzo di una determinata base giuridica per un certo trattamento. In particolare, si evidenzia come l'**interesse legittimo** (ex art. 6 par. 1 lett. f) del GDPR) costituisca una base giuridica utilizzabile per attività di trattamento dati necessarie all'innovazione in ambito IA, purché sia effettuato il

[2] TIM non condivide la posizione espressa.

corretto bilanciamento con i diritti e le libertà degli interessati, come chiarito anche da un recente parere dell'European Data Protection Board.

Inoltre, l'obbligo di raccogliere il consenso genitoriale per gli infra-quattordicenni e la verifica della capacità di consenso per i minori tra i 14 e i 18 anni rischiano di imporre ai fornitori di sistemi IA oneri gestione del consenso sproporzionati, soprattutto se applicati indiscriminatamente a tutte le tipologie di sistemi IA.

Art. 5 (Principi in materia di sviluppo economico)

L'**articolo 5, comma 1 lett. d)** riguarda il possibile indirizzamento delle piattaforme di e-procurement della PA a privilegiare soluzioni IA con data center nazionali per i dati strategici.

Osservazioni

La disposizione merita particolare attenzione. Si ricorda che il testo iniziale della lett. d) prevedeva un riferimento a "dati critici" (categoria di dati più estesa rispetto ai dati strategici) e una formulazione generalmente più prescrittiva sul *procurement* della Pubblica Amministrazione. L'esame parlamentare su questo punto è stato complesso, volto a evitare l'introduzione di criteri che potessero creare disparità ingiustificate tra fornitori o ostacoli non proporzionati. **La formulazione finale approvata dal Senato, che fa riferimento a "dati strategici" e utilizza l'espressione "possano essere privilegiate", rappresenta un compromesso accettabile** che bilancia le esigenze di indirizzo pubblico con la necessità di non precludere l'accesso a soluzioni tecnologiche avanzate. Tale equilibrio andrebbe mantenuto**.**

Si conferma tuttavia la criticità derivante dalla successiva introduzione dell'articolo 6, comma 2, che, come già evidenziato, impone un obbligo generalizzato di localizzazione in netto contrasto con l'approccio più e proporzionato qui adottato.

Art. 6 (Disposizioni in materia di sicurezza e difesa nazionale)

Il comma 2 dell'art. 6, introdotto al Senato, stabilisce che i sistemi di IA "**destinati all'uso in ambito pubblico**" debbano essere installati su server ubicati nel

territorio nazionale, ad eccezione di quelli impiegati in operazioni militari all'estero, al fine dichiarato di tutelare la "sovranità e la sicurezza dei dati sensibili dei cittadini

Osservazioni[3]

La formulazione del comma 2 presenta diverse criticità:

- **Definizione dell'ambito di applicazione**: l'espressione "uso in ambito pubblico" è eccessivamente generica e si presta a interpretazioni estensive che vanno ben oltre le finalità di sicurezza nazionale richiamate dalla rubrica dell'articolo. Difatti, un'interpretazione ampia di questa locuzione comporterebbe l'imposizione di obblighi di localizzazione indiscriminati a un vasto numero di soggetti, incluse le Pubbliche Amministrazioni per qualsiasi sistema di IA, ma anche soggetti privati che erogano servizi di interesse pubblico (es. trasporti, energia, acqua) o che utilizzano IA in spazi pubblici (es. videosorveglianza). Ciò avverrebbe anche per sistemi che non trattano dati strategici per la sicurezza nazionale, limitando fortemente l'accesso alle migliori tecnologie disponibili sul mercato e ostacolando il processo di sviluppo tecnologico della PA, in contrasto con gli obiettivi della Strategia nazionale sull'IA.
- **Conflitto con la normativa UE:** l'obbligo generalizzato di localizzazione nazionale non è previsto dall'AI Act e appare in potenziale contrasto con i principi fondamentali del mercato unico relativi alla libera circolazione dei dati (Art. 1 GDPR) e dei servizi (Direttiva Servizi), rischiando di introdurre restrizioni ingiustificate e frammentare il mercato digitale europeo.
- **Non coerenza interna con il DDL:** la disposizione del comma 2 è incoerente con l'**articolo 5**, lettera d) che, per gli appalti pubblici, si limita a suggerire una mera preferenza per soluzioni con localizzazione nazionale solo per i *dati strategici*, senza imporre alcun obbligo generalizzato. Tale previsione appare disallineata anche rispetto all'approccio seguito dall'Agenzia per la Cybersicurezza Nazionale in materia di qualificazione dei servizi cloud per la PA.

Si ritiene che l'obbligo di localizzazione nazionale indiscriminato creerebbe barriere all'ingresso per molti fornitori di soluzioni IA avanzate, limiterebbe la

[3] TIM non condivide la posizione espressa.

scelta della PA, potrebbe compromettere la continuità operativa di servizi esistenti (e già utilizzati dalle amministrazioni pubbliche) e avrebbe ripercussioni negative sulla competitività e l'efficienza del sistema economico nel suo complesso. L'obbligo di localizzazione, peraltro, interviene in modo disarmonico rispetto alle Linee guida sull'adozione di sistemi di IA nella PA che AgID è in procinto di adottare, creando così ulteriore incertezza giuridica.

Per queste ragioni si propone di **modificare il comma 2** specificando che l'obbligo di localizzazione nazionale dei server si applica **esclusivamente** ai sistemi di intelligenza artificiale impiegati per le attività di sicurezza nazionale, cybersicurezza e difesa nazionale definite al comma 1 dello stesso **articolo 6**.

In subordine, qualora non fosse possibile intervenire direttamente sul testo in sede legislativa, si ritiene necessaria l'adozione di un atto interpretativo formale che chiarisca la limitazione dell'ambito di applicazione del comma 2 alle sole finalità di sicurezza nazionale, escludendo un'applicazione generalizzata all'intero "ambito pubblico".

Art. 16 (Delega al Governo in materia di dati, algoritmi e metodi matematici per l'addestramento di sistemi di intelligenza artificiale)

L'**articolo 16** conferisce al Governo una delega per adottare, entro dodici mesi, uno o più decreti legislativi volti a definire una disciplina organica sull'utilizzo di dati, algoritmi e metodi matematici per l'addestramento dei sistemi di IA. La delega include criteri per individuare ipotesi specifiche, diritti e obblighi, strumenti di tutela (risarcitori/inibitori) e sanzioni, attribuendo le controversie alle sezioni specializzate in materia di impresa.

Osservazioni

La finalità e la necessità di tale delega appaiono poco chiare, data l'esistenza di un quadro normativo europeo già complesso e in via di attuazione (AI Act, GDPR, Direttiva Copyright, Data Act, Data Governance Act) che già incide significativamente sulla disciplina dei dati e degli algoritmi utilizzati per l'addestramento.

Esiste un rischio concreto che l'esercizio di questa delega porti all'introduzione di normative nazionali specifiche e potenzialmente più restrittive o comunque divergenti rispetto a quanto previsto dall'AI Act e dalla normativa europea collegata.

Ciò contrasterebbe direttamente con il principio stabilito all'**articolo 3, comma 5** del presente DDL, secondo cui non si devono introdurre obblighi aggiuntivi rispetto all'AI Act.

Si suggerisce di considerare la **soppressione dell'articolo 16** per evitare il rischio di creare incertezza giuridica rispetto ad un quadro UE già corposo.

In alternativa andrebbero **circoscritti in modo più preciso l'oggetto e i criteri direttivi**, vincolando il Governo a legiferare solo su aspetti non coperti dalla disciplina unionale e strettamente necessari per l'ordinamento nazionale.

Art. 25 (Tutela del diritto d'autore delle opere generate con l'ausilio dell'intelligenza artificiale)

L'**articolo 25** interviene sulla legge 22 aprile 1941, n. 633 (Legge sul diritto d'autore), specificando all'art. 1 che la tutela riguarda le opere dell'ingegno "umano", anche se create con l'ausilio di strumenti IA, purché risultato del lavoro intellettuale dell'autore. Introduce inoltre l'articolo 70-septies, che consente, nei limiti degli articoli 70-ter e 70-quater della stessa legge e nel rispetto della Convenzione di Berna, la riproduzione ed estrazione di dati da opere accessibili per finalità di addestramento di modelli IA (Text and Data Mining - TDM).

Osservazioni

La formulazione attuale dell'**articolo 25** è il risultato di significative revisioni avvenute durante l'esame in prima lettura, volte a recepire il complesso equilibrio tra la tutela del diritto d'autore e le esigenze di sviluppo dell'intelligenza artificiale, in coerenza con il quadro normativo europeo. In particolare, attraverso il richiamo agli articoli 70-ter e 70-quater della Legge sul diritto d'autore, la norma conferma correttamente l'applicazione dell'eccezione per il Text and Data Mining (TDM) all'addestramento dei modelli IA, prevedendo per i titolari dei diritti la possibilità di riservare l'utilizzo delle proprie opere (cd. *opt-out*), meccanismo pienamente

conforme a quanto stabilito dalla Direttiva (UE) 2019/790 sul diritto d'autore nel mercato unico digitale.
La disposizione rappresenta un punto di equilibrio fondamentale e delicato, raggiunto dopo un ampio confronto tra i diversi portatori di interesse (titolari dei diritti, sviluppatori di IA, utilizzatori). Il mantenimento di tale equilibrio è essenziale per fornire certezza giuridica e non pregiudicare l'innovazione e l'utilizzo dei modelli di IA nel nostro Paese.

Per questo Anitec-Assinform ritiene che **l'articolo 25, nella sua attuale formulazione, non vada modificato**. Qualsiasi emendamento volto ad alterare questo equilibrio – ad esempio, restringendo l'applicazione dell'eccezione TDM o tentando di sostituire il regime di opt-out previsto dalla normativa europea con un regime di opt-in (richiedendo quindi un consenso preventivo) – creerebbe grave incertezza giuridica. Ciò danneggerebbe la capacità dell'industria nazionale di sviluppare e utilizzare l'IA generativa in condizioni di parità nel contesto europeo, vanificando il complesso lavoro di bilanciamento già svolto dal Senato.

Art. 26 (Modifiche al Codice penale e ad ulteriori disposizioni penali)

L'articolo 26, comma 1, lettera c) introduce un nuovo reato per contrastare la diffusione di contenuti manipolati con l'Intelligenza Artificiale.

Osservazioni

Questa proposta presenta alcune criticità. La definizione del reato è eccessivamente generica e potrebbe penalizzare anche comportamenti legittimi. Non distingue, infatti, tra la semplice condivisione di contenuti generati dall'IA e un loro utilizzo intenzionalmente dannoso o fraudolento. Inoltre, l'ordinamento giuridico attuale dispone già di strumenti, come il reato di diffamazione, che potrebbero essere adattati per affrontare gli abusi legati all'IA.
Per questi motivi, suggeriamo di introdurre nell'articolo un'esenzione dalla responsabilità per i fornitori di servizi online. Questa modifica dovrebbe prevedere che tali fornitori non siano ritenuti responsabili per i contenuti di terzi generati attraverso le loro piattaforme, in quanto il loro ruolo si limita a fornire gli strumenti di intelligenza artificiale, senza poter controllare o determinare il tipo di contenuti che gli utenti decidono di creare o diffondere. Un simile approccio permetterebbe

di bilanciare efficacemente l'esigenza di contrastare gli usi dannosi dell'IA con la tutela dell'innovazione digitale e delle attività legittime online. Questa esenzione dalla responsabilità consentirebbe ai fornitori di servizi di continuare a sviluppare e offrire soluzioni innovative, senza essere esposti a rischi legali sproporzionati per le azioni degli utenti.