

Oggetto: Memoria dell'Istituto Italiano di Intelligenza Artificiale per l'Industria – AI4I

Commissioni riunite IX (Trasporti, poste e telecomunicazioni) e X (Attività produttive, commercio e turismo) della Camera dei deputati – Audizione sullo schema di decreto legislativo recante adeguamento al Regolamento (UE) 2024/1689 **(Atto del Governo n. 421)**

Al4I è l'Istituto Italiano di Intelligenza Artificiale per l'Industria, istituito in attuazione del decreto-legge n. 73 del 2021. L'Istituto opera come soggetto nazionale di ricerca e trasferimento tecnologico e sostiene il sistema produttivo nello sviluppo, nella validazione e nell'adozione di soluzioni di intelligenza artificiale.

Il Regolamento (UE) 2024/1689 è direttamente applicabile; lo schema di decreto legislativo in esame non ne recepisce le disposizioni, ma adegua l'ordinamento nazionale, individua le autorità competenti e disciplina gli strumenti necessari alla sua attuazione. La presente memoria esamina la dimensione tecnico-industriale dell'Atto del Governo n. 421, con particolare riguardo alla governance, agli spazi di sperimentazione e alle condizioni necessarie per rendere gli obblighi dell'AI Act concretamente applicabili da imprese e amministrazioni.

Sintesi delle osservazioni

L'attuazione nazionale dell'AI Act deve essere costruita come infrastruttura di adozione, oltre che come sistema di vigilanza. La conformità può generare fiducia e accesso al mercato quando imprese e amministrazioni dispongono di competenze, standard, servizi di prova, capacità di calcolo, strumenti di valutazione e canali tempestivi di interlocuzione con le autorità. Su questa base, AI4I sottopone all'attenzione delle Commissioni sei indicazioni prioritarie:

- istituire un punto unico di accesso, con istruttorie coordinate tra AgID, ACN, autorità settoriali e Garante per la protezione dei dati personali, senza alterare le rispettive competenze;
- configurare lo Spazio di sperimentazione italiano come un percorso completo, dalla qualificazione regolatoria alla sperimentazione tecnica e alla produzione di evidenze utilizzabili nella valutazione di conformità e nell'accesso al mercato;
- dotare la sandbox di un catalogo minimo di servizi, risorse dedicate e infrastrutture di prova, distinguendo la gratuità della partecipazione agli organi dalla necessità di una capacità tecnica ed esecutiva effettiva;
- presidiare la normazione CEN-CENELEC e definire un fascicolo interoperabile delle evidenze, riutilizzabile nei rapporti con sandbox, organismi notificati, autorità di vigilanza e regolatori settoriali;
- ridurre l'incertezza applicativa dell'articolo 6 dell'AI Act mediante modelli di autovalutazione, orientamenti preventivi non vincolanti e precedenti anonimizzati, senza introdurre una certificazione nazionale parallela;
- collegare la sandbox regolatoria a una facility nazionale, anche organizzata in rete, per la validazione dell'IA industriale e della Physical AI, con capacità di simulazione, prova in condizioni reali, cybersecurity e verifica integrata della sicurezza.

1. Dall'adeguamento normativo a una politica di capacità

Lo schema in esame definisce una parte essenziale della governance italiana dell'intelligenza artificiale: individua le autorità, ne disciplina i poteri, istituisce lo Spazio di sperimentazione italiano e regola il raccordo con autorità settoriali, ricerca e sistema produttivo. La discrezionalità nazionale non riguarda la ridefinizione degli obblighi europei, bensì la qualità dell'architettura istituzionale e degli strumenti di accompagnamento. Il parametro decisivo sarà quindi la capacità del nuovo assetto di ridurre l'incertezza, accelerare l'apprendimento regolatorio e consentire l'integrazione di sistemi affidabili nei processi produttivi e amministrativi.

Il quadro europeo conferma questa impostazione. L'AI Continent Action Plan, il nuovo quadro EuroHPC per le AI Gigafactories, l'Apply AI Strategy e il percorso del Cloud and AI Development Act affiancano alla regolazione investimenti in capacità di calcolo, dati, competenze e adozione settoriale. Il Digital Omnibus on AI, approvato dal Parlamento europeo il 16 giugno 2026 e adottato dal Consiglio il 29 giugno 2026, ha collegato il rinvio degli obblighi sui sistemi ad alto rischio alla disponibilità di standard e strumenti di supporto. Le nuove date - 2 dicembre 2027 per i sistemi ad alto rischio stand-alone e 2 agosto 2028 per quelli incorporati nei prodotti - definiscono una finestra operativa che deve essere utilizzata per costruire procedure, competenze e capacità di prova.

Ne deriva un principio operativo: alla regolazione basata sul rischio deve corrispondere un'attuazione basata sulle capacità. Rientrano in questa nozione le competenze tecniche e giuridiche, le infrastrutture di prova, i dati governati, gli standard, i processi organizzativi, gli strumenti di supervisione e l'accesso a supporto qualificato. La loro assenza trasforma gli obblighi in costi fissi che gravano proporzionalmente di più su PMI e startup e possono rafforzare la concentrazione del mercato. La condivisione di tali capacità rende invece la conformità un fattore di accesso e crescita.

2. Governance nazionale: un solo procedimento, più autorità competenti

Gli articoli 4 e 5 dello schema attribuiscono ad AgID il ruolo di autorità nazionale di notifica e ad ACN il ruolo generale di autorità di vigilanza del mercato, mantenendo le competenze di Banca d'Italia, CONSOB e IVASS nei rispettivi settori e quelle del Garante per la protezione dei dati personali negli ambiti previsti dal Regolamento. L'articolo 12 rafforza inoltre il Comitato di coordinamento presso la Presidenza del Consiglio. L'architettura è coerente con la natura trasversale dell'IA, ma la pluralità di autorità può produrre un costo di coordinamento elevato se non viene accompagnata da processi comuni.

La soluzione consiste in un modello di accesso unico e competenze coordinate: l'impresa presenta una sola istanza, costruisce un solo fascicolo e segue un percorso istruttorio unitario. Le autorità conservano integralmente i propri poteri, operando su una base informativa comune, con un'autorità capofila individuata per ciascun progetto, tempi definiti e attivazione tempestiva dei soggetti competenti.

A tal fine, i decreti attuativi relativi allo Spazio di sperimentazione potrebbero utilmente prevedere:

- un punto unico di accesso e un responsabile del procedimento per ciascun progetto;
- una matrice preventiva delle competenze, che individui autorità capofila, autorità associate e responsabilità istruttorie;

- il principio “once only” per dati, documentazione ed evidenze tecniche già prodotti dal partecipante;
- termini di risposta e modalità di risoluzione dei conflitti interpretativi tra autorità;
- il coinvolgimento necessario del Garante nei progetti che comportano trattamento di dati personali, in coerenza con l’articolo 57, paragrafo 10, dell’AI Act, e delle altre autorità settoriali per i profili di rispettiva competenza;
- linee guida congiunte e una banca dati di orientamenti, quesiti e soluzioni anonimizzate, in modo da trasformare i singoli casi in conoscenza riutilizzabile.

La qualità della governance dipende inoltre dalle risorse. L’assenza di compensi per i componenti degli organi di coordinamento non può equivalere all’assenza di budget per laboratori, prove, valutazioni indipendenti, ambienti sicuri e competenze specialistiche. La sandbox richiede una dotazione operativa propria e la possibilità di acquisire servizi tecnici, altrimenti il procedimento rischia di limitarsi a uno scambio documentale senza effettiva capacità di validazione.

3. Lo Spazio di sperimentazione come filiera regolatoria e industriale

Gli articoli 26-31 costituiscono la parte più innovativa dello schema. La sandbox, tuttavia, non dovrebbe essere interpretata come una deroga alla disciplina né come una forma di autorizzazione anticipata. I partecipanti restano responsabili dei sistemi sperimentati e il rapporto di uscita non equivale a una dichiarazione di conformità. Il valore dello strumento consiste nella produzione guidata di evidenze: ai sensi dell’articolo 57, paragrafo 7, dell’AI Act, l’autorità rilascia una prova scritta delle attività completate e un exit report che devono essere positivamente considerati dalle autorità di vigilanza e dagli organismi notificati, con la possibilità di accelerare in misura ragionevole la successiva valutazione di conformità.

Per assolvere questa funzione, lo Spazio di sperimentazione italiano potrebbe utilmente essere progettato come un percorso integrato dalla qualificazione regolatoria all’accesso al mercato, articolato in quattro fasi e fondato su risultati verificabili:

- Fase 1 – qualificazione e piano di sperimentazione: individuazione del ruolo dell’operatore nella catena del valore, classificazione preliminare del sistema, mappatura della normativa applicabile, definizione delle metriche e dei rischi da verificare;
- Fase 2 – assurance tecnica e organizzativa: verifica della governance dei dati, della documentazione, dell’accuratezza, della robustezza, dei bias, della cybersecurity, della tracciabilità, della supervisione umana e dei meccanismi di continuità e fallback;
- Fase 3 – prova in condizioni reali controllate: sperimentazione con limiti di autonomia, soglie di arresto, gestione degli incidenti, monitoraggio del drift e possibilità di isolamento o sostituzione dei componenti critici;
- Fase 4 – uscita e accesso al mercato: predisposizione di un fascicolo di evidenze, exit report, piano di monitoraggio post-deployment e raccordo con organismo notificato, autorità di settore o procedura di procurement, secondo il caso.

Il fascicolo prodotto potrebbe utilmente essere modulare e interoperabile. Le evidenze già acquisite non dovrebbero essere ricostruite in ogni passaggio. Un fascicolo comune delle evidenze di conformità, aggiornabile lungo il ciclo di vita, ridurrebbe i costi di transazione e renderebbe concretamente applicabile il principio di proporzionalità.

L'esperienza spagnola offre un'indicazione utile. La prima sandbox nazionale ha ricevuto 44 candidature e selezionato 12 sistemi ad alto rischio in ambiti diversi, combinando dialogo con il regolatore, test operativi e validazione dei requisiti. Il valore pubblico dello strumento risiede anche nella produzione di metodi, guide e soluzioni riutilizzabili dall'intero ecosistema. Questa esternalità di conoscenza giustifica l'accesso gratuito e prioritario per PMI e startup, poiché il beneficio supera quello del singolo progetto.

I criteri di selezione potrebbero utilmente considerare la maturità tecnologica, il valore di apprendimento regolatorio, la replicabilità dei risultati, l'addizionalità del sostegno pubblico, la rilevanza per le filiere strategiche, la qualità del partenariato tra fornitore e utilizzatore finale e la possibilità di produrre strumenti condivisibili. Il portafoglio dei progetti deve evitare sia la concentrazione sui soggetti già meglio attrezzati sia l'ammissione di iniziative troppo immature per generare evidenze utili.

4. Standard, conformità, evidenze

Una parte sostanziale dell'AI Act sarà resa operativa attraverso standard armonizzati, linee guida e codici di condotta. Il progetto prEN 18286, relativo al sistema di gestione della qualità ai fini dell'AI Act, è entrato in consultazione nell'ottobre 2025; CEN e CENELEC hanno successivamente accelerato i lavori per recuperare i ritardi. Per i modelli di IA per finalità generali, il Codice di condotta pubblicato dall'AI Office il 10 luglio 2025 e approvato il 1° agosto 2025 articola gli obblighi in materia di trasparenza, diritto d'autore e sicurezza dei modelli con rischio sistemico.

La normazione tecnica incide direttamente sulla struttura del mercato. Gli standard determinano le prove richieste, i costi fissi sostenuti dagli operatori e le architetture più agevolmente conformi. Una disciplina costruita prevalentemente sui processi dei grandi fornitori può risultare formalmente aperta e, al tempo stesso, difficilmente accessibile alle imprese più piccole e ai sistemi industriali verticali.

Si propone pertanto di affiancare alla governance regolatoria un presidio nazionale della normazione tecnica, in raccordo con UNI, CEI e la rappresentanza italiana nei tavoli CEN-CENELEC, con quattro compiti:

- coordinare la partecipazione di industria, PMI, ricerca e pubbliche amministrazioni ai lavori europei;
- tradurre gli standard in modelli documentali, liste di controllo, protocolli di prova e strumenti utilizzabili dagli operatori;
- raccogliere dalle sandbox evidenze sui requisiti difficili da applicare e riportarle nei processi europei di normazione e revisione;
- assicurare che test, benchmark e dossier prodotti in Italia siano compatibili con gli standard europei e spendibili anche in contesti transfrontalieri.

La sandbox, la normazione e la valutazione di conformità potrebbero utilmente condividere una stessa architettura delle evidenze. Ogni requisito potrebbe utilmente essere collegato a una misura, a un protocollo di prova, a un responsabile e a un'evidenza conservabile. Il passaggio dalla conformità dichiarata alla conformità dimostrabile riduce il rischio di un adempimento prevalentemente documentale.

5. Il nodo dell'articolo 6: certezza ex ante senza una certificazione parallela

La classificazione dei sistemi ad alto rischio rimane uno dei principali nodi applicativi. L'articolo 6 segue due percorsi: i sistemi collegati alla normativa di armonizzazione dei prodotti di cui all'Allegato I e le categorie di utilizzo elencate nell'Allegato III. Nel secondo caso, i paragrafi 3 e 4 consentono al fornitore di ritenere che il sistema non presenti un rischio significativo quando svolge funzioni limitate, procedurali, preparatorie o di miglioramento di attività umane già completate, imponendo però una valutazione documentata. Nel primo caso, la nozione di componente di sicurezza può risultare difficile da applicare a software modulari, aggiornabili e inseriti in sistemi complessi.

L'incertezza ha effetti economici concreti: ritarda gli investimenti, incentiva classificazioni eccessivamente prudenti, aumenta il costo della consulenza e può spingere le imprese a rinunciare ai casi d'uso più innovativi. Al tempo stesso, una interpretazione nazionale vincolante non potrebbe modificare il perimetro uniforme stabilito dal Regolamento europeo.

Una nuova asseverazione nazionale si sovrapporrebbe alla valutazione di conformità e potrebbe frammentare il mercato interno. Risulta preferibile un meccanismo di supporto preventivo, trasparente e privo di effetti autorizzatori, composto da:

- un modello standard per la valutazione documentata prevista dall'articolo 6, paragrafo 4;
- alberi decisionali ed esempi settoriali, aggiornati con le linee guida della Commissione e con gli sviluppi dell'Allegato III;
- la possibilità di richiedere un orientamento motivato alle autorità competenti, con tempi definiti e fermo restando il potere di vigilanza;
- una corsia di accesso alla sandbox per i casi di classificazione incerta o di confine;
- la pubblicazione di precedenti anonimizzati e la segnalazione tempestiva degli effetti delle modifiche europee sugli investimenti in corso.

Il fornitore continuerebbe ad assumere la responsabilità della classificazione, ma potrebbe farlo su una base informativa più prevedibile. In questo modo si riduce il rischio di contenzioso ex post senza creare un livello nazionale di autorizzazione non previsto dall'AI Act.

6. Dalla sandbox regolatoria alla validazione dell'Industrial e Physical AI

La Physical AI comprende sistemi che percepiscono l'ambiente e producono azioni con effetti fisici: robot industriali e collaborativi, macchine autonome, sistemi logistici, impianti e dispositivi cyberfisici. In questi casi il rischio è una proprietà dell'intero sistema e deriva dall'interazione tra software, sensori, attuatori, rete, operatori umani e ambiente operativo. L'Italia dispone di una base manifatturiera, meccatronica e robotica che può trasformare questa traiettoria tecnologica in vantaggio industriale, purché siano disponibili ambienti nei quali progettare, testare e validare soluzioni prima della diffusione su scala.

La validazione richiede una verifica integrata del sistema, che comprenda sicurezza funzionale, cybersecurity, robustezza rispetto a condizioni non previste, deriva delle prestazioni e attacchi, supervisione umana, meccanismi di arresto e recupero operativo. La sola accuratezza del modello non fornisce un livello di assurance sufficiente.

Servono simulazioni e gemelli digitali, prove hardware-in-the-loop, ambienti robotici, test avversariali, valutazioni dell'interazione uomo-macchina e sperimentazioni controllate in condizioni reali.

Si propone pertanto di collegare lo Spazio di sperimentazione italiano a una Facility nazionale di validazione dell'IA industriale, eventualmente organizzata come rete di infrastrutture specializzate con un nodo centrale di coordinamento. La facility potrebbe utilmente mettere a disposizione:

- capacità HPC e ambienti on-premise o segregati per dati e modelli sensibili;
- piattaforme di simulazione, digital twin e testbed per robotica, automazione e sistemi autonomi;
- servizi di valutazione dei modelli, test avversariali, cybersecurity, analisi dei bias, robustezza e monitoraggio della deriva delle prestazioni;
- protocolli di prova coerenti con standard europei, normativa di prodotto e requisiti dell'AI Act;
- supporto alla transizione dal prototipo all'industrializzazione e all'adozione, soprattutto per PMI e filiere manifatturiere.

La distinzione dei ruoli deve restare netta. Le autorità definiscono il piano di sperimentazione, esercitano la vigilanza e rilasciano gli atti previsti dal Regolamento; la facility produce e documenta evidenze tecniche secondo protocolli verificabili; gli organismi notificati svolgono, quando prevista, la valutazione di conformità. Questa separazione consente la cooperazione senza confondere assistenza tecnica, vigilanza e certificazione.

AI4I, in ragione del mandato istituzionale e delle competenze nell'IA industriale, è disponibile a contribuire alla definizione e all'operatività della rete, nonché a supportare il Comitato di coordinamento e il Gruppo operativo previsti dagli articoli 27 e 28, secondo le modalità individuate dalle autorità competenti e nel rispetto delle rispettive funzioni.

Infine, giova qui segnalare una specifica iniziativa di AI4I volta a favorire la conoscenza e l'adozione delle soluzioni di intelligenza artificiale da parte delle PMI italiane: si tratta del cd. SUK, una piattaforma di scouting e validazione delle soluzioni di IA e di sostegno all'incontro tra domanda e offerta, che mette in condizioni gli utilizzatori, per lo più piccole e medie aziende, di focalizzare le proprie esigenze e scoprire le possibili soluzioni, ed offre ai produttori sia supporto tecnico e risorse di calcolo per la validazione dei propri prodotti, sia una visibilità di mercato.

Lo sviluppo di sandbox normative e tecniche potrebbe utilmente integrarsi con una simile piattaforma e contribuire all'implementazione di un modello di trasferimento tecnologico innovativo.

7. Proposte puntuali

In estrema sintesi, si sottopongono le considerazioni seguenti:

- Operatività anticipata. Rendere operativo lo Spazio di sperimentazione italiano prima del termine europeo del 2 agosto 2027, utilizzando la fase iniziale per definire procedure, capacità e primi casi pilota.
- Catalogo dei servizi. Prevedere, nei decreti di cui agli articoli 27 e 28, un catalogo minimo che comprenda qualificazione regolatoria, governo dei dati, valutazione dei rischi, test di robustezza e cybersecurity, verifica dei bias e della supervisione umana, prove in condizioni reali, relazione di uscita e supporto al percorso di conformità.

- **Coordinamento automatico.** Integrare le disposizioni sulla sandbox assicurando il coinvolgimento del Garante per i progetti che trattano dati personali e delle autorità settoriali per i profili di competenza, secondo un procedimento a ingresso unico.
- **Risorse e capacità tecnica.** Distinguere la gratuità della partecipazione agli organi dalla necessità di risorse dedicate per prove, laboratori, consulenze specialistiche e ambienti sicuri; consentire accordi con enti di ricerca e strutture di prova selezionati secondo criteri trasparenti.
- **Fascicolo interoperabile.** Stabilire che documentazione ed evidenze prodotte nella sandbox siano strutturate in un formato riutilizzabile nella valutazione di conformità, nella vigilanza, nel procurement e nei procedimenti settoriali.
- **Trasparenza dei risultati.** Integrare l'articolo 31 con indicatori relativi a tempi di accesso, numero e dimensione dei partecipanti, costi, progetti completati, riduzione del tempo di accesso al mercato, incidenti, strumenti prodotti e riutilizzo degli apprendimenti; pubblicare guide e risultati anonimizzati.
- **Normazione tecnica.** Istituire un presidio nazionale coordinato per i lavori CEN-CENELEC e per l'attuazione del Codice di condotta sui modelli di IA per finalità generali, con adeguata rappresentanza di PMI, industria e ricerca.
- **Supporto sull'alto rischio.** Prevedere modelli, orientamenti non vincolanti e precedenti anonimizzati per l'applicazione dell'articolo 6, fermo restando che la responsabilità della classificazione e i poteri delle autorità rimangono quelli stabiliti dal diritto europeo.
- **Facility di validazione.** Promuovere un'infrastruttura nazionale, anche organizzata in rete, per la validazione dell'IA industriale e della Physical AI, collegata alla sandbox e distinta dalle funzioni di vigilanza e certificazione.
- **Cooperazione europea.** Utilizzare l'articolo 29 per orientare fin dall'inizio la sandbox italiana al mutuo riconoscimento delle evidenze, ai progetti transfrontalieri e al raccordo con l'AI Office e con la futura sandbox europea.

Conclusioni

L'Atto del Governo n. 421 può porre le basi di un sistema nazionale capace di coniugare tutela, innovazione e competitività. La governance potrà utilmente organizzare un percorso operativo comprensibile; la sandbox potrà disporre di capacità di prova e produrre evidenze riutilizzabili; gli standard potranno utilmente essere presidiati come parte della politica industriale; la classificazione del rischio potrà essere accompagnata da strumenti preventivi; la Physical AI richiede ambienti sperimentali coerenti con la natura sistemica dei rischi associati.

La qualità dell'attuazione dipenderà dalla praticabilità tecnica, dalla proporzionalità e dalla possibilità di accumulare e riutilizzare conoscenza. La condivisione di evidenze, competenze e infrastrutture consente alla tutela dei diritti di sostenere l'adozione e alla competitività di svilupparsi entro un quadro affidabile.