DB non solo diritto bancario

leggi l'articolo nel sito www.dirittobancario.it

ATTUALITÀ

# Intelligenza artificiale: primo via libera del Governo ai decreti attuativi

11 Giugno 2026

**Alessandro Ferrari**, Partner, Head of Technology Sector, DLA Piper

**Alessandro Ferrari**, Partner, Head of Technology Sector, DLA Piper

**Alessandro Ferrari**

Alessandro Ferrari è Partner del dipartimento Intellectual Property & Technology e dirige il Sector Technology in Italia e si occupa principalmente di diritto applicato alla tecnologia, assistendo i clienti in questioni transactional, advisory and IT litigation. Ha esperienza nella redazione e negoziazione di accordi strategici e cross-border di outsourcing di processi aziendali e di altri contratti commerciali, IT e relativi alla proprietà intellettuale in diversi settori e in diverse geografie. Ha inoltre esperienza nella consulenza su tutti gli aspetti del processo di sourcing/approvvigionamento, compreso lo sviluppo della struttura dell'accordo, la negoziazione e l'assistenza ai clienti nell'implementazione e nelle strategie di integrazione, nella governance e nei performance management regimes.

Studio Legale Tributario Associato

**DLA Piper**

Il Consiglio dei Ministri del 10 giugno 2026 ha approvato, in esame preliminare, due schemi di decreto legislativo in materia di intelligenza artificiale.

Il primo schema riguarda i poteri delle autorità nazionali, la vigilanza, le sanzioni, gli spazi di sperimentazione e la formazione, e contiene anche disposizioni in materia di lavoro.

Il secondo schema disciplina l'utilizzo dei sistemi di intelligenza artificiale nelle attività di polizia e introduce disposizioni in materia di responsabilità civile e penale.

Il punto da chiarire subito è che non si tratta ancora di testi definitivi. Gli schemi sono stati approvati in via preliminare e dovranno completare l'iter previsto, con possibili modifiche prima dell'approvazione finale e della pubblicazione in Gazzetta Ufficiale.

L'intervento si colloca nel quadro della Legge 23 settembre 2025, n. 132, che reca disposizioni e deleghe al Governo in materia di intelligenza artificiale, e del Regolamento UE 2024/1689, ossia l'AI Act. La logica è quella di adeguare l'ordinamento nazionale al quadro europeo, non di creare un regime italiano parallelo o alternativo.

**1. Executive summary**

Il pacchetto approvato dal Governo conferma che la regolazione italiana dell'AI sta entrando in una fase più operativa.

Le aree più rilevanti sono:

- governance nazionale dell'AI Act, con ruolo centrale di AgID e ACN;
- vigilanza, poteri ispettivi e sanzioni;
- sandbox e sperimentazione regolatoria;
- AI nei processi di lavoro e nelle decisioni che incidono sui lavoratori;
- formazione e AI literacy;

**vedi l'articolo online**

- uso dell'AI da parte delle forze di polizia, con disciplina specifica per biometria e riconoscimento facciale;
- responsabilità civile, accesso alle prove e presunzione del nesso causale;
- responsabilità penale e possibile impatto sui modelli 231;
- tutela di dati, algoritmi e metodi di addestramento come segreti commerciali, ove ricorrano i presupposti.

La direzione è chiara: l'AI non viene trattata come una tecnologia isolata, ma come un'infrastruttura organizzativa e decisionale che richiede governance, documentazione, controlli, responsabilità interne e contratti adeguati.

**2. Governance nazionale: AgID, ACN e autorità settoriali**

Secondo lo schema di decreto attualmente disponibile, le autorità nazionali per l'intelligenza artificiale sono AgID e ACN.

AgID opera come autorità nazionale di notifica, con poteri relativi alle procedure di notifica e agli organismi di valutazione della conformità. ACN assume invece un ruolo centrale nella vigilanza del mercato per i sistemi di AI ed è individuata come punto di contatto unico.

Resta fermo il ruolo delle autorità settoriali, in particolare nei settori bancario, finanziario e assicurativo. Lo schema richiama Banca d'Italia, CONSOB e IVASS quali autorità competenti nei rispettivi ambiti, oltre al Garante per la protezione dei dati personali nei limiti delle competenze rilevanti.

Per le imprese regolamentate, questo è un punto essenziale. La compliance AI non sarà solo una questione interna di policy, né soltanto un tema privacy. Potrà coinvolgere, a seconda dei casi, ACN, AgID, Garante Privacy, Banca d'Italia, IVASS, CONSOB e altre autorità competenti.



**3. Sanzioni: allineamento all'AI Act, ma con articolazione nazionale**

Lo schema di decreto prevede un sistema sanzionatorio articolato, coordinato con l'AI Act.

Per le violazioni più gravi, relative alle pratiche vietate dall'art. 5 dell'AI Act, la sanzione può arrivare fino a 35 milioni di euro o, se superiore, fino al 7% del fatturato mondiale totale annuo dell'esercizio precedente. Sono poi previste soglie inferiori per altre categorie di obblighi, inclusi obblighi di provider, deployer, organismi notificati, trasparenza e informazioni alle autorità.

Il dato sanzionatorio è importante, ma non è l'aspetto più rilevante. Il vero punto, per le imprese, sarà la capacità di dimostrare un sistema di controllo effettivo: classificazione dei sistemi AI, ruoli AI Act, documentazione tecnica, logging, human oversight, risk management, gestione degli incidenti, monitoraggio post-deployment e controllo delle modifiche.

In prospettiva, le organizzazioni dovranno poter dimostrare non solo di avere "una policy AI", ma di avere processi verificabili per acquistare, sviluppare, usare, modificare e dismettere sistemi AI.

**4. Lavoro: stop alle decisioni esclusivamente automatizzate**

Uno dei profili più rilevanti riguarda il lavoro.

Lo schema prevede che, nei processi decisionali concernenti il rapporto di lavoro, il datore che utilizza sistemi AI debba assicurare che le decisioni relative alla costituzione, modifica o risoluzione del rapporto, inclusi i provvedimenti disciplinari, non siano adottate unicamente sulla base di un trattamento automatizzato.

La decisione definitiva deve essere riservata a una persona fisica che eserciti un potere effettivo e autonomo.

Il lavoratore avrebbe inoltre diritto a ottenere, su richiesta e mediante intervento umano, una motivazione intelligibile della decisione, inclusa l'indicazione dell'eventuale incidenza del sistema AI sul processo decisionale e dei principali parametri considerati. Lo schema prevede anche la nullità del licenziamento intimato in violazione del divieto di decisione esclusivamente automatizzata.

Questo può incidere su sistemi di recruiting, screening dei candidati, workforce management, performance management, scoring interno, scheduling automatizzato, people analytics, sistemi disciplinari e strumenti di monitoraggio o valutazione della produttività.

Il punto non sarà solo formale. Non basterà dichiarare che "la decisione finale è umana" se, nella pratica, l'output del sistema determina o condiziona in modo sostanziale la decisione. Le imprese dovranno documentare il ruolo dell'intervento umano, la possibilità di contestazione, le logiche decisionali principali, i presidi anti-discriminatori e gli obblighi informativi.

**5. Salute e sicurezza sul lavoro**

Lo schema introduce anche un collegamento espresso tra AI e salute e sicurezza nei luoghi di lavoro. L'utilizzo di sistemi AI che incidono sull'organizzazione del lavoro, sui ritmi produttivi, sulle modalità di esecuzione della prestazione o sui processi decisionali rilevanti ai fini della sicurezza dovrebbe essere valutato nell'ambito della valutazione dei rischi ai sensi del D.Lgs. 81/2008.

I datori di lavoro dovrebbero inoltre assicurare informazione e formazione sui rischi specifici connessi all'utilizzo dei sistemi AI e sulle misure di prevenzione e protezione adottate.

Questo profilo può essere particolarmente rilevante per logistica, manufacturing, retail, piattaforme digitali, sanità, servizi finanziari, contact center e organizzazioni che usano strumenti AI per ottimizzare turni, carichi di lavoro, priorità operative o controlli di performance.

**6. Formazione, AI literacy, università, professioni e PA**

Il primo schema dedica una parte significativa alla formazione. Sono previste misure su scuola, formazione dei docenti, alfabetizzazione degli adulti, riqualificazione professionale, pubblica amministrazione, università, enti di ricerca, AFAM, ITS Academy, amministrazione della giustizia, professioni e sanità.

Per le imprese, il collegamento con l'AI Act è immediato: l'art. 4 dell'AI Act impone a provider e deployer di adottare misure per assicurare un livello sufficiente di AI literacy del personale e delle altre persone che operano o utilizzano sistemi AI per loro conto.

La formazione non dovrebbe quindi essere trattata come un corso generico sull'AI. Dovrà essere differenziata per ruoli: board e management, legal, compliance, privacy, risk, procurement, HR, IT, cybersecurity, data science, business owner e utenti finali.

Il contenuto dovrà cambiare a seconda del tipo di sistema AI utilizzato, del livello di rischio, del processo aziendale interessato e delle persone impattate dagli output.

**7. Polizia, biometria e riconoscimento facciale**

Il secondo schema disciplina l'utilizzo dell'AI da parte delle forze di polizia.

L'impostazione è quella di ammettere l'uso di sistemi AI come strumenti di supporto, con revisione umana qualificata, tracciabilità e rispetto dei diritti fondamentali. Per i sistemi ad alto rischio, la sorveglianza umana deve essere effettiva e conforme all'AI Act.

La disciplina più sensibile riguarda l'identificazione biometrica remota in tempo reale in luoghi pubblici o aperti al pubblico. Lo schema la consente solo per finalità circoscritte, come prevenzione di specifiche minacce o ricerca di persone scomparse o vittime di determinati reati.

Il confronto biometrico deve avvenire su banche dati di riferimento adeguate e lo schema vieta l'uso di banche dati biometriche alimentate, in tutto o in parte, mediante scraping non mirato o costituite in violazione della normativa data protection.

Sono previsti limiti procedurali, temporali e territoriali. L'autorizzazione deve riguardare uno specifico evento o il tempo strettamente necessario, comunque non superiore a quindici giorni, con possibili proroghe motivate.

In caso di mancato rispetto delle condizioni, l'utilizzo deve essere interrotto, i dati e gli output devono essere cancellati e i risultati non possono essere utilizzati.

Nel procedimento penale, lo schema prevede l'intervento del pubblico ministero e del giudice per le indagini preliminari. Il pubblico ministero richiede l'autorizzazione al GIP, che provvede con decreto motivato; sono previste procedure d'urgenza con convalida successiva.

Per i fornitori tecnologici, questo non è un tema solo pubblico. Chi sviluppa o fornisce soluzioni biometriche, video analytics, identity verification, cybersecurity, law enforcement technology o piattaforme di data analytics dovrà valutare con grande attenzione intended purpose, contesto d'uso, limiti contrattuali, audit, logging, accountability e clausole di uso vietato.

**8. Responsabilità penale e modelli 231**

Lo schema introduce una nuova fattispecie penale relativa all'omessa adozione di misure di sicurezza nei sistemi AI e all'alterazione illecita dei sistemi.

La norma riguarda, in particolare, sistemi AI ad alto rischio e condotte come progettazione, addestramento, produzione, immissione sul mercato o utilizzo professionale in assenza di misure tecniche idonee a prevenire malfunzionamenti o alterazioni, oppure in assenza di misure di sorveglianza umana, quando ne derivi un concreto pericolo per vita, incolumità individuale, incolumità pubblica o sicurezza dello Stato.

La bozza prevede anche l'inserimento nel D.Lgs. 231/2001 di fattispecie connesse all'uso di sistemi AI, incluso il nuovo art. 437-bis c.p.; lo schema richiama anche l'art. 612-quater c.p., che andrà valutato separatamente nel testo definitivo.

Questo è un punto di grande rilievo per le imprese. Se confermato nel testo definitivo, la governance AI potrebbe diventare anche un tema 231, almeno per le organizzazioni che sviluppano, addestrano, immettono sul mercato o utilizzano professionalmente sistemi AI ad alto rischio.

I modelli organizzativi dovrebbero quindi considerare presidi su sicurezza, sorveglianza umana, controllo delle modifiche, testing, logging, incident management e tracciabilità delle decisioni tecniche.

**9. Responsabilità civile: accesso alle prove e presunzione del nesso causale**

Sul piano civile, lo schema non sembra introdurre una responsabilità oggettiva generalizzata per l'AI.

La tecnica utilizzata è diversa: rafforzamento degli strumenti probatori del danneggiato, accesso a documentazione rilevante e presunzione relativa del nesso causale in caso di violazione di obblighi previsti dall'AI Act.

In particolare, il giudice potrebbe ordinare l'esibizione di elementi di prova relativi al funzionamento del sistema AI, inclusi registri, documentazione del sistema di gestione dei rischi, documentazione tecnica e informazioni relative ai parametri e alle modalità di supervisione umana.

Lo schema prevede anche tutele per segreti commerciali e informazioni riservate.

È inoltre prevista una presunzione del nesso causale quando il danno deriva dalla violazione di uno o più obblighi dell'AI Act, salva prova contraria. La conformità del sistema AI agli obblighi dell'AI Act, anche se certificata, non esclude di per sé la responsabilità del convenuto.

Per le imprese, questo rafforza l'importanza della documentazione. La domanda pratica diventa: in caso di contestazione, siamo in grado di produrre log, risk assessment, documentazione tecnica, istruzioni d'uso, evidenze di human oversight, test, change log e decisioni di governance?

**10. Assicurazione e azione diretta**

Lo schema contiene anche una disciplina sull'azione diretta nei confronti dell'impresa di assicurazione.

Chi intende promuovere un'azione di risarcimento potrebbe chiedere al soggetto ritenuto responsabile se esiste una copertura assicurativa per la responsabilità civile relativa al danno. In caso di copertura, il danneggiato avrebbe azione diretta nei confronti dell'assicuratore nei limiti del massimale.

Questo profilo è rilevante non solo per il contenzioso, ma anche per la strutturazione dei programmi assicurativi. Le imprese dovrebbero verificare se e come i rischi AI siano coperti da polizze cyber, professional indemnity, product liability, D&O, E&O o altre coperture, e se esistano esclusioni specifiche relative ad algoritmi, modelli, output automatizzati, sistemi high-risk o uso non conforme.

**11. Dati, algoritmi e metodi di addestramento come segreti commerciali**

Un elemento particolarmente interessante per imprese tecnologiche, sviluppatori, provider AI e gruppi industriali è la previsione relativa al Codice della proprietà industriale.

Lo schema prevede che, tra le informazioni aziendali e le esperienze tecnico-industriali tutelabili come segreti commerciali, possano rientrare anche dati, algoritmi e metodi matematici per l'addestramento di sistemi AI, ove ricorrano i presupposti di legge.

Sono richiamati, in particolare, architetture dei modelli, funzioni di ottimizzazione, procedure e configurazioni di addestramento e altri elementi tecnico-computazionali funzionali allo sviluppo di sistemi AI.

Se confermata, questa previsione potrà avere impatti rilevanti su contratti di sviluppo AI, licensing, outsourcing tecnologico, partnership di ricerca, joint development, data sharing, procurement e due diligence M&A.

La tutela non sarà automatica: resteranno necessari i requisiti ordinari dei segreti commerciali, inclusa la segretezza, il valore economico derivante dalla segretezza e l'adozione di misure ragionevoli per mantenerla.

**12. Implicazioni operative per le imprese**

Anche prima dell'approvazione definitiva, le imprese dovrebbero iniziare a lavorare su alcune aree prioritarie.

La prima è la mappatura dei sistemi AI. Molte organizzazioni non hanno ancora un inventario affidabile dei sistemi AI in uso, inclusi strumenti embedded in software di terzi, piattaforme HR, CRM, cybersecurity, analytics, procurement, document automation, customer service e strumenti generativi usati dai dipendenti.

La seconda è la classificazione dei sistemi. Occorre distinguere tra pratiche vietate, sistemi high-risk, sistemi soggetti a obblighi di trasparenza, general-purpose AI e strumenti a rischio più contenuto. Questa classificazione deve essere documentata e aggiornata nel tempo.

La terza è il procurement tecnologico. I contratti AI non dovrebbero essere trattati come normali contratti software o SaaS. Servono clausole su ruolo AI Act, intended purpose, documentazione tecnica, istruzioni d'uso, dati, output, IP, logging, audit, cybersecurity, incident management, modifica del sistema, retraining, fine-tuning, subfornitori, cooperazione con le autorità e allocazione della responsabilità.

La quarta è la governance interna. Legal, compliance, privacy, cyber, procurement, HR, risk, IT e business owner devono avere ruoli chiari. L'AI governance non può essere lasciata solo all'IT o alla funzione innovation.

La quinta è il lavoro. Gli strumenti che incidono su recruiting, valutazione, performance, misure disciplinari, licenziamento, organizzazione del lavoro o sicurezza devono essere oggetto di una revisione specifica.

La sesta è la documentazione probatoria. La futura gestione del rischio AI dipenderà anche dalla capacità di produrre evidenze: log, risk assessment, test, validazioni, human oversight, istruzioni, controlli sui dati, change log, incident report e decisioni di governance.

La settima è la formazione. L'AI literacy deve essere concreta, differenziata per ruolo e collegata ai sistemi effettivamente usati dall'organizzazione.

**13. Conclusione**

Il Governo ha avviato la fase attuativa nazionale dell'AI Act. I decreti non sono ancora definitivi, ma indicano chiaramente la direzione della regolazione italiana: l'AI dovrà essere governata attraverso un sistema integrato di compliance, cybersecurity, data protection, controllo dei fornitori, responsabilità interna, formazione, documentazione e tracciabilità.

Per le imprese, il tema non è soltanto "essere compliant" quando i decreti entreranno in vigore. Il tema è arrivare preparate: sapere dove l'AI viene usata, da chi, con quali fornitori, in quali processi, con quali dati, con quali impatti sulle persone, con quale supervisione umana, con quali evidenze documentali e con quale allocazione contrattuale delle responsabilità.

DB non solo diritto bancario

A NEW DIGITAL EXPERIENCE

**dirittobancario.it**