

Novità normativa

AI ACT: IN VIGORE I DECRETI LEGISLATIVI DI ADEGUAMENTO N. 160/2026 E N. 179/2026

Sono entrati in vigore il D.Lgs. 9 settembre 2026, n. 160 (dal 30 settembre) e il D.Lgs. 7 ottobre 2026, n. 179 (dal 23 ottobre), con cui il Governo ha esercitato le deleghe della legge 23 settembre 2025, n. 132 (la «Legge IA») per adeguare l'ordinamento nazionale al Regolamento (UE) 2024/1689 (l'«AI Act»).

Il quadro che ne risulta incide direttamente sulle imprese: sono individuate le autorità di vigilanza e definite sanzioni amministrative fino a 35 milioni di euro o al 7% del fatturato mondiale; viene introdotto il delitto di cui all'articolo 437-*bis* c.p., che entra, unitamente al reato di cui all'art. 612-*quater* c.p., nel catalogo dei reati presupposto del D.Lgs. 231/2001; sono previsti strumenti processuali che agevolano il risarcimento dei danni causati da sistemi di IA.

Per i datori di lavoro, infine, le decisioni relative al rapporto di lavoro non potranno fondarsi unicamente su trattamenti automatizzati, a pena di nullità, e l'impiego dell'IA dovrà essere considerato nella valutazione dei rischi per la salute e la sicurezza.

I due decreti in sintesi

Il **D.Lgs. 160/2026** disciplina l'impiego dell'IA da parte delle Forze di polizia e introduce disposizioni penali sostanziali e processuali in materia di impiego illecito dei sistemi di IA nonché disposizioni processuali civili in materia di risarcimento dei danni; il **D.Lgs. 179/2026** individua le autorità competenti e i relativi poteri, istituisce gli spazi di sperimentazione normativa e detta disposizioni in materia di formazione, lavoro e tutela di dati e algoritmi come segreti commerciali.

Le autorità nazionali competenti e i poteri di vigilanza

Il D.Lgs. 179/2026 conferma e precisa l'assetto delineato dalla Legge IA:

— l'Agenzia per l'Italia digitale (**AgID**) è l'autorità di notifica, competente per la valutazione, la designazione, la notifica e il monitoraggio degli organismi di valutazione della conformità;

— l'Agenzia per la cybersicurezza nazionale (**ACN**) è l'autorità di vigilanza del mercato sui sistemi di IA e il punto di contatto unico con le istituzioni dell'Unione Europea. Ad ACN, in particolare, sono altresì attribuiti poteri ispettivi e sanzionatori, oltre alle funzioni di promozione e sviluppo dell'IA per i profili di cybersicurezza;

— **Banca d'Italia, CONSOB e IVASS** sono autorità di vigilanza del mercato, ciascuna nel proprio ambito, per i sistemi di IA ad alto rischio utilizzati nei servizi bancari, finanziari e assicurativi;

— il **Garante per la protezione dei dati personali** è competente limitatamente ai casi previsti dall'articolo 74, paragrafo 8, dell'AI Act (tra cui i sistemi ad alto rischio impiegati a fini di contrasto, di gestione delle frontiere e di amministrazione della giustizia).

Il coordinamento è affidato al "Comitato di coordinamento" istituito presso la Presidenza del Consiglio dei ministri e ad accordi tra le autorità.

Il sistema sanzionatorio

L'articolo 23 del D.Lgs. 179/2026 prevede, salvo che il fatto costituisca reato, sanzioni amministrative pecuniarie che, se superiori all'importo fisso, sono parametriche al fatturato mondiale totale annuo dell'esercizio precedente:

- **fino a 35 milioni di euro o al 7%**, per le pratiche di IA vietate dall'articolo 5 dell'AI Act;
- **fino a 15 milioni di euro o al 3%**, per l'inosservanza, tra l'altro, degli obblighi relativi ai sistemi ad alto rischio e ad altri obblighi specifici (tra cui gli articoli 16, 22-26, 31, 33-34, 50, 73 e 80 del AI Act);
- **fino a 7,5 milioni di euro o all'1%**, per la fornitura di informazioni inesatte, incomplete o fuorvianti agli organismi notificati o alle autorità;
- **fino a 1 milione di euro o allo 0,5%**, per la violazione degli obblighi minori relativi alla valutazione d'impatto sui diritti fondamentali (art. 27 dell'AI Act) e al diritto alla spiegazione dei singoli processi decisionali (art. 86 dell'AI Act).

Ai sensi dell'art. 22, co.1, del D.Lgs. 179/2026 per le violazioni di scarsa offensività o pericolosità le autorità possono adottare misure non pecuniarie (ordini di cessazione, dichiarazioni pubbliche).

Per le PMI, comprese le microimprese, e per le start-up innovative le sanzioni sono determinate secondo criteri agevolati.

I provvedimenti sanzionatori sono pubblicati, in linea di principio, per estratto sul sito dell'autorità (in forma anonima solo in ipotesi specifiche).

Gli spazi di sperimentazione normativa

È istituito lo Spazio di sperimentazione italiano per l'IA (*regulatory sandbox*), gestito congiuntamente da AgID e ACN, in cui fornitori e potenziali fornitori possono sviluppare e testare i propri sistemi in un ambiente controllato, con priorità per PMI e start-up; criteri di ammissione e regole di funzionamento saranno definiti con

decreto congiunto delle due Agenzie. Sono previsti anche spazi dedicati ai sistemi impiegabili in chiave duale e all'attività giudiziaria, spazi regionali o locali e il raccordo con la sperimentazione FinTech.

Intelligenza artificiale e rapporto di lavoro

Di particolare rilievo per le imprese è l'articolo 41 del D.Lgs. 179/2026: il datore di lavoro che si avvale di sistemi di IA deve assicurare che le decisioni finali relative alla costituzione, alla modificazione o alla risoluzione del rapporto di lavoro — inclusi i provvedimenti disciplinari e le valutazioni delle prestazioni — non siano adottate unicamente sulla base di un trattamento automatizzato. La decisione definitiva spetta a una persona fisica dotata di un potere effettivo e autonomo.

Il consenso del lavoratore non vale a derogare a tale regola e il licenziamento in violazione delle regole sopra riportate è **nullo**.

L'articolo 42 richiede inoltre di considerare, nella valutazione dei rischi ai sensi dell'articolo 28 del D.Lgs. 81/2008, l'impiego di sistemi di IA che incidono sull'organizzazione del lavoro, sui ritmi produttivi, sulle modalità della prestazione o sui processi decisionali rilevanti per la sicurezza, e di informare e formare i lavoratori sui rischi specifici e sulle misure adottate.

Il nuovo reato di cui all'articolo 437-bis c.p. e la responsabilità degli enti

Il D.Lgs. 160/2026 introduce nel codice penale il delitto di «*Omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale e alterazione illecita dei sistemi*». Si tratta di un reato di pericolo, che si configura nelle seguenti ipotesi:

- l'**omessa adozione** delle misure tecniche di sicurezza previste per la progettazione, l'addestramento, la produzione e l'immissione sul mercato di sistemi di IA **ad alto rischio**, idonee a prevenirne malfunzionamenti o alterazioni, ovvero delle misure di sorveglianza umana, quando ne derivi un

pericolo per la vita o per l'incolumità pubblica o individuale (reclusione da uno a cinque anni) o per la sicurezza dello Stato (da due a otto anni);

— le medesime condotte commesse per **colpa grave**, con pena ridotta da un terzo a un sesto;

— l'**alterazione** di sistemi di IA ad alto rischio, salvo che il fatto costituisca più grave reato (reclusione da due a sei anni ovvero, in caso di pericolo per la sicurezza dello Stato, da tre a dieci anni);

— l'omissione **intenzionale** delle misure di sorveglianza umana da parte dell'utilizzatore professionale (*deployer*) di sistemi ad alto rischio, punita con le pene previste per la prima ipotesi.

Il D.Lgs. 160/2026 inserisce altresì nell'elenco dei reati presupposto del D.Lgs. 231/2001 il nuovo articolo 25-*vicies*, rubricato "*Reati commessi con l'uso di sistemi di intelligenza artificiale*", che estende la responsabilità dell'ente al delitto di cui all'articolo 437-*bis* c.p. e a quello di illecita diffusione di contenuti generati o alterati con sistemi di IA (c.d. *deepfake*), di cui all' art. 612-*quater* c.p. (introdotto dalla Legge IA). In entrambi i casi si applicano, oltre alle sanzioni pecuniarie, le sanzioni interdittive previste dall'articolo 9, comma 2, lettere b), c), d) ed e) del D.Lgs. 231/2001.

Il risarcimento dei danni cagionati da sistemi di IA

Il D.Lgs. 160/2026 introduce strumenti processuali a favore di chi agisce per il risarcimento di danni, contrattuali o extracontrattuali, cagionati nell'utilizzo di un sistema di IA.

Presunzione del nesso causale. Se il danno deriva dalla violazione di obblighi previsti dall'AI Act, il nesso di causalità tra violazione e danno è presunto, salvo prova contraria.

Azione diretta contro l'assicuratore. Prima di agire, il danneggiato può chiedere al presunto responsabile se sia coperto da un'assicurazione

della responsabilità civile, con risposta dovuta entro trenta giorni; può inoltre agire direttamente contro l'impresa di assicurazione, nei limiti del massimale.

Dati, algoritmi e modelli come segreti commerciali.

Il **D.Lgs. 179/2026** aggiunge all'articolo 98 del Codice della proprietà industriale il comma 1-bis: i dati, gli algoritmi e i metodi matematici per l'addestramento dei sistemi di IA sono tutelabili come informazioni aziendali riservate quando ricorrano i medesimi *requisiti di segretezza* previsti dal comma 1.

Formazione, professioni ed equo compenso

Il **D.Lgs. 179/2026** introduce novità anche per gli ordini e i collegi professionali. I percorsi di formazione iniziale e continua dovranno includere moduli su funzionamento e limiti dei sistemi di IA, sulla relativa disciplina giuridica e sui profili deontologici, tra cui gli obblighi informativi verso il cliente, con un monte ore minimo per ciascun periodo formativo. I consigli nazionali degli ordini e dei collegi dovranno adeguare i propri regolamenti entro sei mesi dall'entrata in vigore del decreto, ossia entro il 23 aprile 2027. Regole analoghe valgono per le professioni non regolamentate e, attraverso il sistema ECM, per le professioni sanitarie.

L'uso dell'IA potrà, inoltre, incidere sull'**equo compenso** del professionista: entro dodici mesi i parametri ministeriali, compresi quelli forensi, dovranno essere integrati con criteri di modulazione legati alla classificazione di rischio del sistema impiegato.

Sono previste, infine, iniziative di alfabetizzazione per scuola, università, pubblica amministrazione e giustizia (per i magistrati, tramite la Scuola superiore della magistratura) e un piano, finanziato fino a 100 milioni di euro, contro l'uso eccessivo e non consapevole dei social media e degli ambienti basati sull'IA da parte degli studenti.

Le azioni raccomandate

Alla luce delle novità illustrate si raccomanda eventualmente di valutare, in particolare, di:

- censire i sistemi di IA sviluppati, acquistati o utilizzati, qualificando il ruolo dell'impresa (fornitore, *deployer*, importatore o distributore) e la classe di rischio di ciascun sistema;
- verificare l'assenza di pratiche vietate dall'articolo 5 dell'AI Act;
- rivedere i processi di gestione del personale che impiegano strumenti di IA, garantendo e documentando la decisione finale umana;
- aggiornare il documento di valutazione dei rischi e la formazione dei lavoratori in relazione ai rischi connessi all'uso dell'IA;
- integrare la mappatura dei rischi-reato e il Modello 231 con i delitti di cui agli articoli 437-bis e 612-*quater* c.p.;
- adottare misure di segretezza adeguate per dati, algoritmi e modelli.

Per richieste di approfondimento è possibile contattare i professionisti riportati in calce.

ULTERIORI INFORMAZIONI SU QUESTO ARGOMENTO O SU FATTISPECIE CORRELATE POSSONO ESSERE RICHIESTE A:

Dipartimento Compliance SLM

Responsabile: avv. Selene Sontacchi

Autore: avv. Andrea Ferrari

+39 0461 23100 – 260200 – 261977

ss@slm.tn.it

DISCLAIMER

Le Newsletter di SLM rappresentano uno strumento di informazione gratuito a disposizione di tutti coloro che siano interessati a riceverle (newsletter@slm.tn.it). Le Newsletter di SLM non possono in alcun caso essere considerate pareri legali, né possono essere ritenute idonee a risolvere casi specifici in assenza di una preventiva valutazione della fattispecie concreta da parte di un legale.

Il presente contributo è aggiornato al 26 ottobre 2026 e ha finalità meramente informativa.

Le informazioni riportate potrebbero pertanto non essere attuali al momento della lettura.

Per visionare il testo integrale dell'informativa privacy aggiornata (ex art. 13 Regolamento UE 2016/679) ed aggiornare i tuoi dati accedi al link: <https://slm.tn.it/notizie/newsletter>.

CANCELLAZIONE DEL SERVIZIO

Chi avesse ricevuto o ricevesse le Newsletter di SLM per errore oppure desiderasse non ricevere più comunicazioni di questo tipo in futuro o comunque intendesse revocare il consenso prestato al trattamento può in ogni momento cliccare sul link "Annulla iscrizione", presente in calce ad ogni email inviata, e seguire le istruzioni che verranno presentate.

In alternativa, per chiedere la cancellazione e/o per segnalare eventuali problemi tecnici, è sempre anche possibile scrivere, senza particolari formalità, un'email a: segreteria@slm.tn.it.