POLICY BRIEF

POLLICINO & PARTNERS
AIDVISORY

D.Lgs. 160/2026: anticipazione dell'alto rischio?

Oreste Pollicino[1] e Rebecca Pupella[2]

Con il Digital Omnibus sull'IA sono state differite le date di applicazione di una parte significativa della disciplina relativa ai sistemi ad alto rischio. In particolare, ai sensi dell'art. 113 dell'AI Act, le disposizioni del capo III, sezioni 1, 2 e 3, ad eccezione dell'art. 6, par. 5, si applicheranno: (i) dal 2 dicembre 2027, per i sistemi classificati ad alto rischio ai sensi dell'art. 6, par. 2, e dell'Allegato III e (ii) dal 2 agosto 2028, con riferimento ai sistemi classificati ad alto rischio ai sensi dell'art. 6, par. 1, e dell'Allegato I.

Il differimento riguarda, tra l'altro, le disposizioni relative alla gestione dei rischi e dei dati (artt. 9 e 10), alla documentazione tecnica e alla registrazione dei log (artt. 11 e 12), alla trasparenza e alle istruzioni d'uso (art. 13), alla sorveglianza umana (art. 14), ai requisiti di accuratezza, robustezza e cybersicurezza (art. 15), nonché al sistema di gestione della qualità (art. 17).

L'entrata in vigore, il 30 settembre 2026, del d.lgs. 9 settembre 2026, n. 160 richiede tuttavia, tra le altre cose, di coordinare tali scadenze con la disciplina nazionale in materia di responsabilità civile e penale connessa all'impiego dell'intelligenza artificiale.

La lettura congiunta delle disposizioni nazionali e del regolamento europeo consente, infatti, di individuare due profili che assumono particolare rilievo per le organizzazioni: (i) l'anticipazione sostanziale dell'adozione di alcuni presidi propri dei sistemi ad alto rischio e (ii) l'estensione della rilevanza organizzativa e probatoria di tali presidi anche ai sistemi che non rientrano nella categoria dell'alto rischio.

L'art. 12 e l'anticipazione sostanziale dei presidi di sicurezza e sorveglianza umana

L'art. 12 del d.lgs. 160/2026 introduce nel codice penale l'art. 437-bis, rubricato "*Omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale e*

---

[1] Managing Partner, Pollicino AIdvisory.

[2] Advisor AI Governance & Cybersicurezza, Pollicino AIdvisory.

info@orestepollicino.eu
https://pollicinoaidvisory.eu/

alterazione illecita dei sistemi". Il primo comma dell'articolo dispone: "*Chiunque omette di adottare le misure tecniche di sicurezza, previste per la progettazione, l'addestramento, la produzione, l'immissione sul mercato di sistemi di intelligenza artificiale ad alto rischio, idonee a prevenire malfunzionamenti o alterazioni del funzionamento dei sistemi ovvero omette di adottare misure di sorveglianza umana è punito con la reclusione da uno a cinque anni, quando da tali omissioni derivi pericolo per la vita o l'incolumità pubblica o individuale. Qualora dal fatto derivi un pericolo per la sicurezza dello Stato, la pena è della reclusione da due a otto anni*".

La disposizione attribuisce quindi rilevanza penale all'omessa adozione di determinate misure tecniche di sicurezza e di sorveglianza umana relative ai sistemi ad alto rischio, subordinando la punibilità alla ricorrenza degli ulteriori elementi della fattispecie e, in particolare, al pericolo per i beni giuridici espressamente individuati. I presidi richiamati presentano una convergenza sostanziale con quelli disciplinati dagli artt. 14 e 15 dell'AI Act: l'art. 14 prevede che i sistemi ad alto rischio siano progettati e sviluppati in modo da consentire una sorveglianza umana effettiva durante il loro utilizzo, con misure commisurate ai rischi, al livello di autonomia e al contesto d'uso e l'art. 15 riguarda invece i requisiti di accuratezza, robustezza e cybersicurezza che tali sistemi devono soddisfare lungo il proprio ciclo di vita.

È quindi evidente che vi sia una coesistenza tra una fattispecie penale nazionale già vigente e disposizioni europee relative a presidi sostanzialmente corrispondenti, la cui applicazione è stata differita. È in questo senso che può prospettarsi un'anticipazione sostanziale di alcuni presidi dell'alto rischio: nella misura in cui determinate misure risultino già dovute e la loro omissione possa integrare la fattispecie nazionale, le organizzazioni sono chiamate a valutarne l'adozione prima delle scadenze europee.

Per le organizzazioni, questa distinzione comporta la necessità di affiancare alla pianificazione dell'adeguamento europeo una valutazione delle responsabilità nazionali già applicabili.

Gli artt. 16 e 17 e la rilevanza dei presidi documentali oltre l'alto rischio

Un secondo profilo emerge, nel sistema italiano, dalla disciplina dell'accesso alle prove nei giudizi risarcitori per responsabilità contrattuale ed extracontrattuale. L'art. 16, comma 1, stabilisce che le disposizioni dell'art. 17 si applicano alle azioni di risarcimento del danno, sia contrattuale sia extracontrattuale, cagionato

nell'utilizzo di "*un sistema di intelligenza artificiale*", senza circoscrivere l'ambito applicativo ai sistemi classificati ad alto rischio.

L'art. 17 del decreto, al comma 1, prevede che il giudice, su istanza della parte che allega di avere subito il danno e in presenza degli elementi richiesti dalla norma, ordini all'altra parte o al terzo che ne dispone l'esibizione degli elementi di prova specificamente pertinenti relativi al funzionamento del sistema di IA. Il comma 2 individua espressamente tra tali elementi:

"*a) i registri di cui all'articolo 12 del regolamento (UE) 2024/1689;*

b) la documentazione relativa al sistema di gestione dei rischi di cui all'articolo 9 del regolamento (UE) 2024/1689;

c) le informazioni pertinenti contenute nella documentazione tecnica di cui all'articolo 11 del regolamento (UE) 2024/1689;

d) le informazioni relative ai parametri e alle modalità di supervisione umana di cui all'articolo 14 del regolamento (UE) 2024/1689".

Il coordinamento tra le due disposizioni evidenzia una differenza significativa tra l'ambito delle controversie interessate e le categorie documentali espressamente richiamate. L'art. 16 individua un perimetro che comprende i danni cagionati nell'utilizzo di sistemi di IA indipendentemente dalla loro classificazione come ad alto rischio, mentre l'art. 17 menziona presidi documentali propri dell'alto rischio.

Il decreto induce quindi a riconsiderare le implicazioni della classificazione del rischio sul piano della governance. La classificazione europea conserva la propria funzione nell'individuazione degli obblighi di conformità, ma non esaurisce la valutazione delle informazioni pertinenti ai fini dell'accertamento della responsabilità: quando l'utilizzo di un sistema diviene oggetto di contenzioso, i presidi documentali previsti dall'AI Act per i sistemi ad alto rischio possono assumere rilievo probatorio anche rispetto a sistemi che non rientrano in tale categoria.

Nel sistema italiano, pur in assenza di un obbligo generalizzato di formazione dei documenti, l'art. 17 produce una conseguenza operativa rilevante: in ottica cautelativa, l'organizzazione ha interesse a valutare preventivamente quali evidenze siano necessarie per ricostruire il funzionamento e l'utilizzo dei propri sistemi, anziché rinviare tale verifica al momento in cui insorga una controversia. La predisposizione di una documentazione proporzionata e l'individuazione dei

soggetti che dispongono delle informazioni pertinenti possono agevolare l'adempimento dell'ordine giudiziale e consentire una più compiuta rappresentazione delle circostanze rilevanti.

Le implicazioni per la governance delle imprese

La lettura sistematica proposta individua due effetti differenti, accomunati dalla necessità di valutare la governance dell'IA anche alla luce della disciplina nazionale ora in vigore. Quanto ai sistemi ad alto rischio, l'art. 12 richiede di considerare la rilevanza attuale delle omissioni relative alla sicurezza e alla sorveglianza umana, nei limiti della fattispecie penale e previa individuazione delle misure concretamente esigibili. Quanto agli altri sistemi, gli artt. 16 e 17 rendono rilevante la possibilità di ricostruirne il funzionamento in giudizio, attraverso una disciplina dell'accesso alle prove che richiama espressamente categorie documentali proprie dell'alto rischio.

Per le imprese, ne deriva l'opportunità di affiancare al percorso di adeguamento alle scadenze europee una valutazione già attuale: (i) delle misure di sicurezza e controllo richieste dalla disciplina nazionale applicabile, (ii) delle evidenze necessarie a documentare il funzionamento e l'utilizzo dei sistemi e (iii) delle modalità attraverso le quali rendere disponibili tali informazioni in caso di contestazione, secondo criteri di pertinenza e proporzionalità.

L'anticipazione e l'estensione qui prospettate riguardano, pertanto, la rilevanza sostanziale dei presidi di governance, che può precedere l'applicazione delle corrispondenti disposizioni europee o assumere rilievo oltre la categoria dell'alto rischio. Entro questi limiti, il d.lgs. 160/2026 offre alle organizzazioni una ragione per riesaminare sin d'ora le proprie scelte di controllo e documentazione, mantenendo distinti gli adempimenti giuridicamente dovuti dalle misure adottate in funzione cautelativa e probatoria. In questo quadro, la contrattualistica assume un ruolo sempre più rilevante nel definire gli obblighi informativi e documentali, le modalità di cooperazione in caso di contenzioso e le responsabilità delle parti. Ciò vale soprattutto quando il fornitore è stabilito fuori dall'Italia e non sia direttamente assoggettato alla disciplina nazionale, rendendo opportuno assicurare per via contrattuale la disponibilità delle informazioni e della documentazione necessarie.