

Roberto Sammarchi
Avvocato specialista in diritto dell'informazione, della comunicazione digitale e della protezione dei dati personali, Socio AIAS

Art. 437-bis c.p.: la nuova norma penale sull'IA arriva prima degli standard

Dal 30 settembre 2026 il codice penale contiene un nuovo delitto dedicato alla sicurezza dei sistemi di intelligenza artificiale ad alto rischio. L'art. 437-bis, rubricato «Omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale e alterazione illecita dei sistemi», è stato introdotto dall'art. 12 del D.Lgs. 9 settembre 2026, n. 160 (G.U. n. 214 del 15 settembre 2026), che adegua l'ordinamento al Regolamento (UE) 2024/1689 (AI Act) in attuazione della Legge 132/2025. La collocazione parla da sola alla comunità della prevenzione.
La nuova norma segue immediatamente l'art. 437, rimozione od omissione dolosa di cautele contro infortuni sul lavoro, tra i delitti contro l'incolumità pubblica. Il legislatore estende così la logica delle cautele antinfortunistiche dalla protezione fisica di macchine e impianti alla dimensione algoritmica.

La struttura del reato

— Il *primo comma* punisce con la reclusione da uno a cinque anni chi omette le misure tecniche di sicurezza "previste" per la progettazione, l'addestramento, la produzione e l'immissione sul mercato di sistemi ad alto rischio, idonee a prevenire malfunzionamenti o alterazioni, ovvero omette le misure di sorveglianza umana. Il fatto è punito se ne deriva un pericolo per la vita o l'incolumità pubblica o individuale; se il pericolo riguarda la sicurezza dello Stato, la pena sale da due a otto anni.
— Il *secondo comma* colpisce l'alterazione illecita del sistema.
— Il terzo estende la punibilità alla colpa grave, con pena ridotta.
— Il quarto riguarda l'utilizzatore professionale – il deployer, nel lessico dell'AI Act – che omette intenzionalmente le misure di sorveglianza umana: è la disposizione che tocca più da vicino il datore di lavoro, se introduce sistemi ad alto rischio nei processi aziendali.
— Il delitto entra infine nel catalogo del D.Lgs. 231/2001 con il nuovo art. 25-vicies, che prevede la sanzione pecuniaria da 600 a 1000 quote oltre alle sanzioni interdittive.

Una norma già operativa, parametri tecnici ancora incompleti

Il nodo è temporale: la fattispecie è in vigore, ma i riferimenti tecnici che dovrebbero riempirne il contenuto non sono ancora stabili.
Il Digital Omnibus, pubblicato in Gazzetta ufficiale UE nel luglio 2026, ha rinviato l'applicazione dei requisiti per i sistemi ad alto rischio al 2 dicembre 2027 per quelli dell'Allegato III e al 2 agosto 2028 per quelli integrati nei prodotti dell'Allegato I. Tra questi ultimi rientrano le macchine, cioè proprio l'ambito in cui il rischio infortunistico è più immediato.

Le norme armonizzate affidate al CEN-CENELEC JTC 21, poi, non sono complete. A luglio 2026 risultava approvata soltanto la EN 18286 sul sistema di gestione della qualità; gestione del rischio (prEN 18228) e cybersicurezza (prEN 18282) erano ancora in bozza. Senza citazione in GUUE, nessuna offre presunzione di conformità utilizzabile ai fini difensivi in ambito penale.
Ne deriva un problema di certezza del diritto. Il testo parla di misure "previste" senza precisare "dal regolamento". Il giudice dovrà quindi stabilire quali cautele fossero esigibili, e in base a quale fonte, valutando ex post condotte tenute in assenza di parametri condivisi.

Linee guida sull'alto rischio e sandbox: strumenti di certezza

In questo vuoto, due strumenti dell'AI Act acquistano un peso che va oltre la loro natura di soft law o di regime sperimentale.
Le linee guida della Commissione sulla classificazione ex art. 6, pubblicate in bozza il 19 maggio 2026 e sottoposte a consultazione fino al 23 giugno, chiariscono con esempi pratici quando un sistema è ad alto rischio. In chiave penale incidono sul presupposto del reato e sull'elemento soggettivo: se l'agente poteva riconoscere la natura del sistema, il margine per invocare l'errore si riduce.
La sandbox regolamentare dell'art. 57 offre un ambiente controllato in cui sviluppare, addestrare e testare sistemi sotto la supervisione dell'autorità. In Italia il nuovo decreto legislativo sui poteri delle autorità nazionali (D.Lgs. 179/2026) istituisce lo Spazio di sperimentazione italiano per l'IA, affidato ad AgID e ACN; il Digital Omnibus ha spostato al 2 agosto 2027 il termine per rendere operative le sandbox nazionali.
Il perimetro va però chiarito. Chi partecipa in buona fede è esente da sanzioni amministrative, ma resta responsabile secondo il diritto dell'Unione e nazionale: la sandbox non neutralizza il 437-bis. Il percorso documentato all'interno della sandbox – piano concordato, prova scritta delle attività, relazione di uscita – costituirà tuttavia una prova robusta di diligenza.



Buone prassi e linee guida: il contributo dei professionisti della sicurezza

Il D.Lgs. 81/2008 conosce già la risposta a questo tipo di vuoto. Accanto alle norme tecniche, riconosce buone prassi e linee guida (art. 2, lett. u, v e z) come riferimenti della diligenza esigibile, e affida alla Commissione consultiva permanente la validazione delle buone prassi. Lo stesso schema può operare per l'IA: in assenza di standard armonizzati, prassi documentate, condivise e verificabili diventano il parametro con cui misurare la condotta.
I professionisti rappresentati da AIAS, e a livello europeo da ENSHPO, sono i soggetti naturali per costruirle, perché presidiano il punto in cui il sistema incontra il lavoratore.

Gli ambiti prioritari per il contributo dei professionisti sono i seguenti:

- sorveglianza umana nei processi produttivi: chi la esercita, con quali poteri di intervento e arresto, con quale tracciabilità;
- integrazione dei sistemi ad alto rischio nella valutazione dei rischi e nel DVR, con la consultazione dell'RLS;
- competenza e formazione di chi supervisiona (art. 26 AI Act);
- gestione di anomalie, quasi-incidenti e disattivazioni;
- raccordo tra modello organizzativo ex art. 30 D.Lgs. 81/2008 e presidi 231 per il nuovo art. 25-vicies.

Queste prassi possono alimentare la sandbox, come luogo in cui verificarle su casi reali.

Una presenza già costruita

AIAS ed ENSHPO sono stati presenti in tutti i livelli di consultazione, europei e nazionali, che hanno portato all'attuale definizione del quadro normativo: dall'AI Act e dai suoi strumenti attuativi alla legge 132/2025 e ai decreti che ne sono seguiti. Quel patrimonio di competenza e di presenza istituzionale è la base per un passo ulteriore: un tavolo tecnico sulla sorveglianza umana nei luoghi di lavoro, le cui buone prassi siano sottoposte a validazione istituzionale e verificate nello Spazio di sperimentazione italiano.

La norma penale è arrivata prima degli standard. Il vuoto non si colma aspettando: sarà nella posizione migliore chi potrà documentare cautele ragionevoli, condivise e verificabili. È la logica dell'art. 2087 c.c., la massima sicurezza tecnologicamente possibile, che i professionisti della prevenzione applicano da sempre.

