GIURISPRUDENZA PENALE

# Intelligenza artificiale: in arrivo nuovi reati e nuove responsabilità per gli enti.

di ***Federica Rinaldini***

**Sommario. 1**. Premessa. – **2**. I nuovi reati presupposto ai sensi del D.Lgs. n. 231/2001. – **3**. Il nuovo art. 437-*bis* c.p. - Omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale e alterazione illecita dei sistemi. – **3.1.** L'omessa adozione dolosa di misure tecniche di sicurezza o di misure di sorveglianza umana. – **3.2.** L'alterazione di sistemi di intelligenza artificiale ad alto rischio. – **3.3.** L'omessa adozione di misure tecniche di sicurezza o di misure di sorveglianza colposa. – **4**. L'art. 612-*quater* c.p. - Illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale. – **5**. Confini di rilevanza penale e impatto sui Modelli organizzativi.

## 1. Premessa.

L'intelligenza artificiale sta per entrare ufficialmente nel catalogo dei reati presupposto del D.Lgs. n. 231/2001.

Le nuove disposizioni in materia di intelligenza artificiale scaturiscono dalle deleghe contenute nella Legge 23 settembre 2025, n. 132, adottata nel quadro dell'adeguamento dell'ordinamento nazionale al Regolamento (UE) 2024/1689 (*AI Act*).

Il Consiglio dei ministri ha approvato in via definitiva, il 4 agosto 2026, lo schema di decreto legislativo di adeguamento della normativa nazionale all'*AI Act*, che prevede, tra l'altro, l'introduzione del nuovo art. 437-*bis* c.p. e del nuovo art. 25-*vicies* del D.Lgs. n. 231/2001, con l'inserimento delle relative fattispecie nel catalogo dei reati presupposto 231[1].

Le novità sono particolarmente rilevanti perché vengono introdotte nel sistema 231 fattispecie penali specificamente costruite intorno all'utilizzo e alla sicurezza dei sistemi di intelligenza artificiale.

## 2. I nuovi reati presupposto ai sensi del D.Lgs. n. 231/2001.

Lo schema di decreto prevede l'introduzione, nel D.Lgs. n. 231/2001, del nuovo art. 25-*vicies*, rubricato *"Reati commessi con l'uso di sistemi di*

[1] Il testo definitivo del decreto approvato il 4 agosto 2026 non risulta ancora pubblicato in Gazzetta Ufficiale, le osservazioni del presente contributo sono riferite allo schema trasmesso alle Camere, salvo le modifiche espressamente comunicate dal Governo all'esito dell'approvazione definitiva. Si veda il seguente link.

*intelligenza artificiale"*, che disciplina l'applicazione della responsabilità dell'ente in relazione a due nuove fattispecie:

- l'art. 437-*bis* c.p. – Omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale e alterazione illecita dei sistemi;
- l'art. 612-*quater* c.p. – Illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale.

Il nuovo art. 25-*vicies* prevede, in particolare, per l'art. 437-*bis* c.p., una sanzione pecuniaria da 600 a 1.000 quote; per l'art. 612-*quater* c.p., una sanzione pecuniaria da 200 a 700 quote.

Per entrambe le fattispecie sono inoltre previste sanzioni interdittive, tra cui la *sospensione o revoca di autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito, il divieto di contrattare con la Pubblica Amministrazione, l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e il divieto di pubblicizzare beni o servizi*. In osservanza del principio di proporzionalità, non è stata prevista la misura dell'interdizione dall'esercizio dell'attività, privilegiando le misure incidenti sull'operatività dell'ente nei settori connessi all'illecito, evitando la sanzione integralmente paralizzante dell'attività.

Si tratta di un ampliamento del catalogo 231 di particolare rilievo, anche sotto il profilo delle possibili conseguenze sull'operatività dell'ente, come verrà di seguito illustrato.

## 3. Il nuovo art. 437-*bis* c.p. – Omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale e alterazione illecita dei sistemi.

Il nuovo reato verrà introdotto nel Titolo VI del Codice penale, dedicato ai delitti contro l'incolumità pubblica e, più precisamente, tra i delitti di comune pericolo mediante violenza (artt. 422-437 c.p.), collocandosi subito dopo l'art. 437 c.p. (rimozione od omissione dolosa di cautele contro infortuni sul lavoro).

### 3.1. L'omessa adozione dolosa di misure tecniche di sicurezza o di misure di sorveglianza umana.

La fattispecie prevista dal primo comma contempla un'ipotesi di reato omissivo di pericolo concreto che punisce chi:

- nella progettazione, addestramento, produzione, immissione sul mercato, utilizzazione professionale di sistemi di *intelligenza artificiale ad alto rischio*
- omette di adottare le misure tecniche di sicurezza idonee a prevenire malfunzionamenti o alterazioni del funzionamento del sistema
- ovvero omette le necessarie misure di sorveglianza umana
- qualora dal fatto derivi un pericolo concreto per la vita o l'incolumità individuale ovvero per l'incolumità pubblica o per la sicurezza dello Stato.

La rilevanza penale di tali condotte riguarda specificamente i sistemi di intelligenza artificiale ad alto rischio.
I sistemi di intelligenza artificiale ad alto rischio non sono definiti dal Codice penale; è pertanto necessario fare riferimento all'art. 6 del Regolamento (UE) 2024/1689 (*AI Act*). In particolare, ai sensi di tale norma, un sistema di IA è considerato ad alto rischio, a prescindere dal fatto che sia immesso sul mercato o messo in servizio indipendentemente rispetto ai prodotti di cui alle lettere a) e b) dell'art. 6, qualora siano soddisfatte entrambe le seguenti condizioni:
**"***a) il sistema di IA è destinato a essere utilizzato come componente di sicurezza di un prodotto***,** *o il sistema di IA è esso stesso un prodotto, disciplinato dalla normativa di armonizzazione dell'Unione elencata nell'Allegato I;*
*b) il prodotto, il cui componente di sicurezza a norma della lettera a) è il sistema di IA, o il sistema di IA stesso in quanto prodotto, è soggetto a una valutazione della conformità da parte di terzi ai fini dell'immissione sul mercato o della messa in servizio di tale prodotto, a norma della normativa di armonizzazione dell'Unione elencata nell'Allegato I".*
Ai sensi dell'art. 6, par. 2, sono inoltre considerati ad alto rischio i sistemi di IA di cui all'Allegato III, fermo restando quanto previsto dal par. 3 della medesima disposizione. Quest'ultimo esclude infatti dalla qualificazione di alto rischio, al ricorrere delle condizioni stabilite, i sistemi dell'Allegato III che non presentino un rischio significativo di danno alla salute, alla sicurezza o ai diritti fondamentali delle persone fisiche, anche in ragione della loro limitata incidenza sul risultato del processo decisionale. La deroga non opera, tuttavia, per i sistemi che effettuano la profilazione di persone fisiche, che sono sempre considerati ad alto rischio.
Tra i casi d'uso individuati dall'Allegato III rientrano, a titolo meramente esemplificativo e non esaustivo, sistemi di IA impiegati in ambito biometrico, nelle infrastrutture critiche, nell'istruzione, nell'occupazione e nella gestione dei lavoratori, nell'accesso a servizi essenziali, nel *law enforcement*, nella gestione della migrazione e delle frontiere, nell'amministrazione della giustizia e nei processi democratici.
La qualificazione di un sistema come "ad alto rischio" non può tuttavia essere desunta esclusivamente dal settore di utilizzo, ma richiede una verifica puntuale delle caratteristiche, della finalità e delle concrete modalità di impiego del singolo sistema, anche alla luce delle specifiche condizioni ed eccezioni previste dall'art. 6 dell'*AI Act*. Ne consegue che anche un'impresa operante in un settore estraneo a quelli tradizionalmente associati all'alto rischio può rientrare nell'ambito della fattispecie, qualora utilizzi un sistema qualificabile come ad alto rischio. Ad esempio, una società industriale o commerciale che impieghi un sistema di IA per analizzare e filtrare candidature o per valutare i candidati nell'ambito dei processi di selezione

del personale potrebbe utilizzare un sistema rientrante tra quelli ad alto rischio ai sensi dell'art. 6 e dell'Allegato III dell'AI Act.
Si evidenzia che il testo approvato in via definitiva il 4 agosto 2026 è stato modificato rispetto a quello esaminato in via preliminare dal Consiglio dei ministri il 10 giugno 2026, con la previsione di una disciplina autonoma per la posizione dell'utilizzatore professionale di sistemi di IA ad alto rischio che ometta intenzionalmente di adottare misure di sorveglianza umana[2].
L'elemento oggettivo del reato non si esaurisce nella mera omissione delle misure di sicurezza. È infatti necessario che dalla condotta derivi un pericolo concreto:

- per la vita o l'incolumità individuale (in tal caso è prevista la reclusione da uno a cinque anni);
- ovvero per l'incolumità pubblica o la sicurezza dello Stato (qui la pena è più elevata, da due a otto anni).

La configurazione della fattispecie come reato di pericolo concreto è molto significativa ai fini della delimitazione dell'applicabilità della norma: non ogni omissione, alterazione, carenza organizzativa, tecnica o procedurale nell'utilizzo di un sistema di intelligenza artificiale ad alto rischio assume automaticamente rilevanza penale. Occorre che la condotta omissiva – oltre a riguardare sistemi di intelligenza artificiale ad alto rischio – sia causalmente collegata alla creazione di una situazione di pericolo per i beni giuridici tutelati.
Tale ipotesi è punibile a titolo di dolo.

### 3.2. L'alterazione di sistemi di intelligenza artificiale ad alto rischio.

Il secondo comma dell'art. 437-*bis* c.p. disciplina la fattispecie commissiva relativa all'alterazione illecita di sistemi di IA ad alto rischio.
La condotta consiste nell'alterare il funzionamento del sistema, al di fuori dei casi disciplinati dal primo comma. Come evidenziato nella relazione illustrativa allo schema di decreto, si tratta di una "*previsione di chiusura*", necessaria per evitare aree di impunità nei casi in cui il pericolo concreto derivi dalla manipolazione attiva, esterna, del sistema.
Anche in questo caso la responsabilità penale è subordinata alla produzione di un pericolo concreto per la vita o l'incolumità individuale (pena da due a sei anni) ovvero, nella forma più grave, per l'incolumità pubblica o la sicurezza dello Stato (pena da tre a dieci anni).
Anche per questa seconda fattispecie è richiesto il coefficiente soggettivo del dolo.

[2] Il testo non è ancora stato pubblicato in Gazzetta Ufficiale e il testo integrale definitivo, approvato il 4 agosto 2026, non risulta, allo stato, reperibile in forma consolidata.

**3.3. L'omessa adozione di misure tecniche di sicurezza o di misure di sorveglianza colposa.**

Il legislatore ha previsto la punibilità delle condotte descritte nel primo comma anche a titolo di colpa grave, con riduzione della pena da un terzo a un sesto. Secondo quanto emerge dalla relazione illustrativa allo schema di decreto, la scelta della colpa grave quale soglia di punibilità richiama espressamente il modello dell'art. 590-*sexies* c.p., introdotto dalla legge 8 marzo 2017, n. 24 (c.d. legge Gelli-Bianco) in materia di responsabilità sanitaria.

La rilevanza della colpa grave è particolarmente importante per le imprese perché sposta l'attenzione non soltanto sulle condotte intenzionali, ma anche sulle gravi carenze organizzative, tecniche e di controllo nella gestione dei sistemi di intelligenza artificiale.

Il rischio di incorrere in una sanzione penale o amministrativa ai sensi del D.Lgs. n. 231/2001 non riguarda esclusivamente chi intenzionalmente altera o utilizza in modo illecito un sistema, ma può riguardare anche una gestione gravemente negligente dei presidi di sicurezza e di supervisione.

**4. L'art. 612-*quater* c.p. – Illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale.**

L'art. 612-*quater* c.p., già introdotto dalla Legge n. 132/2025 e attualmente vigente, non costituisce allo stato un reato presupposto ai sensi del D.Lgs. n. 231/2001. Esso è destinato a essere ricompreso nel catalogo dei reati-presupposto attraverso il nuovo art. 25-*vicies* del D.Lgs. n. 231/2001, unitamente al nuovo art. 437-*bis* c.p.

La fattispecie riguarda il fenomeno dei cosiddetti *deepfake*.

Il reato punisce con la reclusione da uno a cinque anni chi:

- cagiona un danno ingiusto a una persona
- cedendo, pubblicando o altrimenti diffondendo
- senza il consenso della persona interessata
- immagini, video o voci falsificati o alterati
- mediante l'impiego di sistemi di intelligenza artificiale
- idonei a indurre in inganno sulla loro genuinità.

La clausola "*altrimenti diffondendo*" indica che il legislatore ha voluto coprire non solo la pubblicazione in senso stretto, ma ogni forma di circolazione del contenuto verso terzi, purché si traduca in una effettiva diffusione.

Non è necessario che il contenuto sia diffuso a un numero elevato di persone: la cessione anche a un singolo terzo può assumere rilievo, purché ricorrano tutti gli ulteriori elementi richiesti dalla fattispecie.

I contenuti diffusi devono avere una idoneità decettiva: la norma non colpisce qualunque contenuto artificialmente generato o modificato, ma quelli che presentano una attitudine ingannatoria, ossia tali da far credere che siano

autentici. Il disvalore oggettivo del fatto, quindi, non è soltanto nella manipolazione tecnica, ma nella sua capacità di simulare la realtà.
A differenza della disposizione di cui all'art. 437-*bis* c.p. che prevede un reato di pericolo, tale ipotesi è stata coniata dal legislatore come un reato di evento: ai fini della consumazione è necessario che si verifichi un danno ingiusto per la persona oggetto della condotta criminosa.
L'elemento soggettivo richiesto dalla norma è quello del dolo.

**5. Confini di rilevanza penale e impatto sui Modelli organizzativi.**
L'ingresso dell'intelligenza artificiale nel catalogo dei reati 231 era solo una questione di tempo. Era prevedibile che l'IA, proprio per la sua capacità di incidere su attività un tempo riservate all'uomo, non potesse restare fuori da questo perimetro.
In relazione all'art. 437-*bis* c.p., il legislatore, opportunamente, non ha optato per una fattispecie onnicomprensiva, capace di sanzionare qualsiasi utilizzo scorretto o negligente di un sistema di intelligenza artificiale: come si legge nell'analisi tecnico-normativa allegata al decreto, la *ratio* legislativa è stata quella di mantenere la coerenza con i principi di legalità, determinatezza, offensività e proporzionalità della risposta sanzionatoria penale.
Il nuovo art. 437-*bis* c.p. – e conseguentemente la responsabilità dell'ente per tale reato – si applica solo ai sistemi di intelligenza artificiale ad alto rischio (nell'accezione tecnica dell'*AI Act*) e richiede che dal fatto derivi la concreta messa in pericolo di beni di rango costituzionale elevato: la vita, l'incolumità individuale o pubblica, la sicurezza dello Stato.
È una scelta di tecnica legislativa che merita di essere sottolineata e la stessa relazione illustrativa allo schema di decreto chiarisce che l'obiettivo è concentrare l'intervento penale sulle violazioni realmente idonee a mettere a repentaglio beni di primaria importanza, non ogni violazione di obblighi regolatori. Gli obblighi derivanti dall'*AI Act* possono tuttavia costituire un parametro rilevante nella valutazione dei presidi organizzativi, tecnici e di supervisione che l'impresa deve adottare per governare il rischio.
Un punto di attenzione, in questo quadro, riguarda la previsione della punibilità ai sensi dell'art. 437-*bis* c.p. a titolo di colpa grave. Il terreno dell'intelligenza artificiale è per sua natura attraversato da incertezza tecnica e da una rapidità evolutiva degli standard che comporta un'oggettiva difficoltà – anche per l'operatore più diligente – di prevedere gli effetti sistemici di un sistema complesso. Assoggettare a sanzione penale qualsiasi errore tecnico avrebbe significato costruire, di fatto, una responsabilità oggettiva, con l'effetto, potenzialmente devastante, di disincentivare l'innovazione e spingere gli operatori più prudenti fuori da un mercato reso ingestibile sul piano del rischio legale.
Si auspica pertanto che l'applicazione giurisprudenziale della fattispecie colposa non si traduca in una lettura troppo estensiva della norma,

consentendo di ravvisare una responsabilità di fatto oggettiva, in aperto contrasto con il principio costituzionale di personalità della responsabilità penale.

Per le imprese, tali novità legislative dovranno tradursi in un messaggio chiaro: la gestione dei sistemi di intelligenza artificiale non può restare confinata all'interno delle sole strutture tecniche, ma richiede una *governance* integrata tra competenze giuridiche, organizzative e tecnologiche.

È tuttavia necessaria una precisazione. Il legislatore ha delimitato l'area di applicazione del nuovo art. 437-*bis* c.p. a determinate condotte poste in essere nell'ambito della progettazione, addestramento, produzione, immissione sul mercato o utilizzazione professionale di sistemi di IA ad alto rischio e, nelle ipotesi previste, richiede altresì la concreta esposizione a pericolo di beni di particolare rilevanza, quali la vita e l'incolumità individuale, l'incolumità pubblica o la sicurezza dello Stato. Ne deriva che il mero utilizzo dell'intelligenza artificiale non costituisce, di per sé, un rischio-reato ai sensi dell'art. 437-*bis* c.p.. Né la circostanza che un'impresa operi in un determinato settore comporta automaticamente che tutti i sistemi di IA da essa utilizzati siano qualificabili come "ad alto rischio".

La verifica deve essere effettuata con riferimento al singolo sistema, alla sua finalità prevista e alle concrete modalità di impiego, secondo i criteri stabiliti dall'art. 6 e dagli Allegati I e III del Regolamento (UE) 2024/1689.

Ciascuna società dovrà valutare se il nuovo rischio rientri o meno nell'ambito delle proprie attività e dei propri processi aziendali. Si tratta, in altri termini, non di un obbligo indistinto di aggiornamento formale del Modello, ma di una verifica di adeguatezza fondata sul concreto *risk assessment* della singola impresa.

La prima attività che le società dovranno porre in essere sarà pertanto la mappatura dei sistemi di IA progettati, addestrati, prodotti, immessi sul mercato o utilizzati e la loro qualificazione alla luce dell'*AI Act*. L'esito di tale valutazione potrà essere diverso da società a società. Qualora, all'esito della mappatura, non siano rinvenibili sistemi qualificabili come ad alto rischio e, conseguentemente, non risulti una concreta esposizione al rischio di commissione della nuova fattispecie, potrà essere sufficiente documentare adeguatamente tale valutazione nell'ambito del *risk assessment*, senza la necessità di introdurre un apparato di procedure specificamente dedicato all'art. 437-*bis* c.p..

Diversamente, in presenza di sistemi di intelligenza artificiale ad alto rischio e attività potenzialmente riconducibili all'ambito della nuova fattispecie, occorrerà valutare l'adeguamento del Modello e dei relativi protocolli, introducendo presidi proporzionati al rischio effettivamente rilevato.

In tal caso, occorrerà individuare con chiarezza ruoli e responsabilità lungo tutta la catena, verificare l'adeguatezza delle misure tecniche di sicurezza e di sorveglianza umana e aggiornare le procedure interne, con particolare

attenzione a sicurezza, supervisione umana, gestione degli incidenti e delle anomalie, controllo dei fornitori, formazione del personale e tracciabilità delle decisioni e dei controlli effettuati. La documentazione dei presidi e dei controlli sarà essenziale anche per poter dimostrare l'effettiva attuazione del Modello ai sensi dell'art. 6 del D.Lgs. n. 231/2001.

Un ulteriore profilo che merita attenzione è il rapporto di tale nuova fattispecie con l'art. 8 del D.Lgs. n. 231/2001, che sancisce l'autonomia della responsabilità dell'ente anche nei casi in cui l'autore del reato non sia stato identificato o non sia imputabile. Il tema può assumere particolare rilievo rispetto ai sistemi di intelligenza artificiale, il cui funzionamento può coinvolgere una pluralità di soggetti e funzioni, tanto interne quanto esterne all'organizzazione. La distribuzione delle attività tra chi sviluppa, fornisce, configura, utilizza e supervisiona il sistema può infatti rendere più complessa l'individuazione del contributo della singola persona fisica alla realizzazione del fatto. In tale contesto, assume ancora maggiore importanza, sul piano organizzativo, una chiara definizione dei ruoli e delle responsabilità, accompagnata da adeguati meccanismi di tracciabilità delle decisioni e dei controlli effettuati.

In definitiva, la selettività della nuova fattispecie penale non è in contrasto con la necessità di una valutazione organizzativa: ne costituisce, piuttosto, il presupposto. Quanto più circoscritta è l'area della rilevanza penale, tanto più l'attività di *risk assessment* deve essere in grado di individuare se, e in quali processi, tale rischio sia concretamente presente, evitando tanto una sottovalutazione del rischio quanto l'introduzione di presidi generalizzati e sproporzionati rispetto all'effettiva esposizione dell'ente.

Diverso è l'impatto sui Modelli organizzativi dell'ingresso nel sistema 231 dell'art. 612-*quater* c.p., che punisce chi cagiona un danno ingiusto a una persona cedendo, pubblicando o altrimenti diffondendo, senza il suo consenso, immagini, video o voci falsificati o alterati mediante l'impiego di sistemi di intelligenza artificiale e idonei a indurre in inganno sulla loro genuinità. Tale reato, a differenza di quello previsto dall'art. 437-*bis* c.p., non è circoscritto ai sistemi di IA ad alto rischio e può pertanto interessare, in linea di principio, un più ampio novero di imprese.

Sotto il profilo 231, sarà quindi necessario verificare, nell'ambito del *risk assessment*, se e come l'IA generativa venga utilizzata nei processi aziendali, con particolare riferimento alla produzione e diffusione di immagini, video e contenuti audio riferibili a persone fisiche. Qualora il rischio risulti concretamente configurabile, il Modello dovrà prevedere presidi proporzionati, come regole sull'utilizzo degli strumenti di IA, individuazione dei soggetti autorizzati alla produzione e pubblicazione dei contenuti, procedure di verifica e approvazione e adeguata formazione del personale. Si dovrà anche porre attenzione ai fornitori esterni a cui sono affidate attività di comunicazione, *marketing* o gestione dei canali digitali, prevedendo, ove

necessario, specifici obblighi contrattuali e meccanismi di controllo. Anche in relazione a tale fattispecie, dunque, l'inserimento del reato nel catalogo 231 non impone un protocollo indistinto per tutte le società, ma richiede una valutazione della concreta esposizione dell'ente al rischio e l'adozione di presidi coerenti con le attività effettivamente svolte.

In questo nuovo scenario si colloca il ruolo dell'Organismo di Vigilanza, la cui funzione resta quella di verificare che il sistema di controllo predisposto dall'ente sia concretamente idoneo a prevenire la commissione dei reati presupposto. È ragionevole attendersi, in questa prospettiva, che i flussi informativi verso l'OdV si arricchiscano progressivamente di elementi quali: la classificazione dei sistemi di IA adottati o in fase di sviluppo; gli incidenti rilevati e le eventuali alterazioni o malfunzionamenti dei sistemi; le modifiche sostanziali apportate ai Modelli nel tempo; le risultanze delle attività di monitoraggio e sorveglianza umana previste dalla normativa.

A questi si affiancano, coerentemente con l'estensione del perimetro di rischio, ulteriori campi che l'Organismo sarà chiamato a presidiare: la verifica dell'adeguatezza della mappatura dei rischi 231 aggiornata ai processi che coinvolgono sistemi di IA ad alto rischio; il controllo sulla formazione erogata al personale coinvolto nella progettazione, addestramento o utilizzo professionale di tali sistemi; la verifica dell'effettivo funzionamento dei canali di segnalazione (anche alla luce della disciplina *whistleblowing*) per anomalie o utilizzi impropri dell'IA.

Resta, però, un nodo da non sottovalutare: l'Organismo di Vigilanza, per composizione tipica, non sempre possiede le competenze tecniche necessarie per valutare l'adeguatezza delle misure di sorveglianza umana ai sistemi di intelligenza artificiale. Il rischio è che la vigilanza si riduca a un adempimento formale, con l'OdV relegato al ruolo di destinatario passivo di informazioni che non è in grado di validare autonomamente. Per evitarlo, l'Organismo di Vigilanza dovrebbe poter contare su flussi informativi strutturati e periodici provenienti dalle funzioni tecniche competenti; in situazioni particolarmente critiche o sensibili, potrebbe valutarsi la nomina di membri con *background* in IA/*data science* o il ricorso strutturato a consulenti esterni; oppure si potrebbero prevedere indicatori di allerta predefiniti e concordati a monte.

In definitiva, il diritto penale ha trovato, almeno sulla carta, un punto di equilibrio tra tutela dei beni giuridici primari e salvaguardia dell'innovazione: la sfida, ora, si sposta alle imprese, chiamate a misurarsi con i nuovi rischi attraverso una puntuale verifica della propria esposizione alle nuove fattispecie introdotte, per tradurre, ove necessario, tale valutazione in adeguati presidi organizzativi e di controllo.