SCLA
STUDIO LEGALE

MODELLO 231: IL NUOVO RISCHIO DA INTELLIGENZA ARTIFICIALE

Avv. Martina Vancini

Con il decreto di adeguamento all'AI ACT il catalogo dei reati presupposto del D.Lgs. 231/2001 si è allungato di una voce: l'art. 25-vicies, dedicato ai delitti commessi impiegando sistemi di intelligenza artificiale.

L'art. 25-vicies non aggiunge uno strumento a reati che c'erano già ma fa del difetto di organizzazione sull'intelligenza artificiale un reato a sé. La sanzione prevista dall'art. 25-vicies è calibrata a quella prevista dall'art. 25-septies: l'omicidio colposo e le lesioni gravi commesse violando la disciplina antinfortunistica. Dunque, un sistema di AI lasciato senza presidi vale, agli occhi della norma, quanto un impianto senza protezioni.

A monte ci sono due reati: il nuovo art. 437-bis c.p. e l'art. 612-quater c.p.

Il nuovo art. 437-bis c.p. sanziona l'omessa adozione delle misure di sicurezza nei sistemi di intelligenza artificiale ad alto rischio e la loro alterazione illecita quando dalla condotta derivi un pericolo concreto per beni di primario rilievo. Invece, l'art. 612-quater c.p. disciplina

la diffusione illecita di contenuti generati o alterati mediante sistemi di intelligenza artificiale (cd. *deepfake*).

Particolare attenzione deve dedicarsi all'art. 437-bis c.p. in cui la rilevanza penale è circoscritta attraverso la riferibilità della condotta ai sistemi di AI ad *alto rischio* e la necessità, nelle ipotesi previste, di un *pericolo concreto per beni giuridici di particolare rilevanza*. La scelta legislativa appare riconducibile alla necessità di evitare che ogni violazione degli obblighi di sicurezza o ogni errore nell'impiego dell'intelligenza artificiale assuma automaticamente rilevanza penale. L'art. 612-quater c.p., invece, non è circoscritto ai soli sistemi ad alto rischio ed è dunque potenzialmente idoneo a coinvolgere una platea più ampia di imprese.

L'inserimento di queste due nuove fattispecie di reato nel sistema 231 non comporta la necessità di adottare un secondo modello e non serve un secondo organismo di vigilanza: serve che il modello esistente contenga una parte speciale sull'intelligenza artificiale, che i protocolli siano scritti in modo da poter essere verificati e che di ogni controllo resti una traccia documentale.

Dovranno quindi innanzitutto essere censiti tutti i sistemi AI in uso e, per ciascuno, dovranno essere individuati: finalità, dati trattati, fornitore, processo su cui incide, persone potenzialmente esposte. Senza questo elenco nessuna delle ulteriori fasi è possibile.

Successivamente, sarà necessario collocare ciascun sistema nelle categorie dell'AI Act: pratica vietata, alto rischio, rischio di trasparenza e rischio minimo. La classificazione va motivata per iscritto perché è il primo documento che verrà chiesto in caso di contestazione.
Dopo di che si dovrà individuare tutte le aree a rischio reato rispetto all'art. 437-bis e all'art. 612-quater e scrivere le procedure che mancano.

Inoltre dovrà essere individuato chi risponde di cosa: referente per l'IA, rapporti con il responsabile della protezione dei dati, con il responsabile del servizio di prevenzione e protezione e con la funzione IT. Le deleghe devono attribuire poteri di spesa e di intervento coerenti con le responsabilità assegnate.

Infine, dovrà essere stabilito che cosa l'Organismo di Vigilanza riceve e con quale periodicità: elenco aggiornato dei sistemi, esiti dei collaudi, registro degli incidenti, esiti degli audit sui fornitori, evidenze della formazione.

Bisogna ricordare che, in sede penale, la differenza tra un'impresa che si salva e una che non si salva risiede nell'esistenza di documenti datati che provano che qualcuno, prima dell'incidente, aveva valutato quel rischio, definito quel controllo e verificato che venisse eseguito.

Il presente articolo non intende fornire un parere legale e, per l'effetto, non può essere considerato sostitutivo di una consulenza legale specifica.

Clicca qui per scaricare l'articolo in PDF