PARTE SPECIALE "F":

VIOLAZIONI IN MATERIA DI AI ACT

relativo al

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

adottato da

CARGO S.r.l.

PREMESSA

Con il Decreto Legislativo 9 settembre 2026, n. 160, recante disposizioni di adeguamento della normativa nazionale al Regolamento (UE) 2024/1689, c.d. "AI Act", il legislatore nazionale è intervenuto, tra l'altro, sul sistema della responsabilità amministrativa degli enti di cui al Decreto Legislativo 8 giugno 2001, n. 231, ampliando il novero dei c.d. reati-presupposto rilevanti ai fini della responsabilità dell'ente.

Il Decreto Legislativo n. 160/2026 è stato pubblicato nella Gazzetta Ufficiale della Repubblica Italiana in data 15 settembre 2026 e le relative disposizioni sono entrate in vigore il 30 settembre 2026 e si inserisce nel più ampio processo di adeguamento dell'ordinamento nazionale alla disciplina armonizzata dell'Unione europea in materia di intelligenza artificiale.

Per quanto di specifico interesse ai fini della presente Parte Speciale, la principale novità introdotta dal Decreto è rappresentata dalla modifica del Decreto Legislativo n. 231/2001; in particolare, l'articolo 15 del D.Lgs. n. 160/2026 ha introdotto nel D.Lgs. n. 231/2001 l'art. 25-vicies, rubricato "**Reati commessi con l'uso di sistemi di intelligenza artificiale**", estendendo la responsabilità dell'ente alle fattispecie di cui agli artt. 437-bis e 612-quater del Codice penale, nei limiti e alle condizioni previste dal medesimo Decreto Legislativo n. 231/2001.

È opportuno, al riguardo, precisare che la mera violazione delle disposizioni contenute nell'*AI Act*, di per sé considerata, non determina l'insorgenza della responsabilità amministrativa dell'ente ai sensi del D.Lgs. n. 231/2001. Tale responsabilità, difatti, può configurarsi esclusivamente laddove la condotta posta in essere non solo integri una delle fattispecie penali espressamente richiamate dall'art. 25-*vicies* ma risponda anche gli ordinari presupposti di imputazione previsti dal D.Lgs. n. 231/2001, ivi compreso il requisito dell'interesse o del vantaggio dell'ente.

REATI COMMESSI CON L'USO DI SISTEMI DI INTELLIGENZA ARTIFICIALE

F.1. LE TIPOLOGIE DEI REATI SOCIETARI DI CUI ALL'ART. 25-*VICES* DEL D.LGS. N. 231/2001

La presente Parte Speciale è volta a illustrare le fattispecie di reato richiamate dall'art. 25-vicies del D.Lgs. n. 231/2001, introdotto dal D.Lgs. n. 160/2026, nonché a individuare, in termini generali, i principali profili di rischio connessi all'utilizzo di sistemi di intelligenza artificiale nell'ambito delle attività dell'ente.

Di seguito si procede, pertanto, a una sintetica descrizione delle fattispecie rilevanti ai fini della responsabilità amministrativa dell'ente.

F.2. REATI COMMESSI CON L'USO DI SISTEMI DI INTELLIGENZA ARTIFICIALE

• ***Omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale e alterazione illecita di sistemi (art. 437-bis cod. pen.)***

La fattispecie di cui all'art. 437-bis c.p. costituisce una delle principali novità introdotte dal legislatore nazionale nell'ambito della tutela penale connessa all'impiego di sistemi di intelligenza artificiale.

La disposizione sanziona, al primo comma, la condotta di chi ometta di adottare le misure tecniche di sicurezza previste in relazione alla progettazione, all'addestramento, alla produzione e all'immissione sul mercato di sistemi di intelligenza artificiale ad alto rischio, qualora tali misure siano idonee a prevenire malfunzionamenti o alterazioni del funzionamento dei sistemi e dall'omissione derivi un pericolo per l'incolumità pubblica o individuale,

La medesima disposizione contempla, altresì, un aggravamento del trattamento sanzionatorio qualora dal fatto derivi un pericolo per la sicurezza dello Stato.

Il secondo comma disciplina, inoltre, la condotta di chi, al di fuori delle ipotesi contemplate dal primo comma, alteri sistemi di intelligenza artificiale ad alto rischio, qualora da tale condotta derivi un pericolo per la vita o per l'incolumità pubblica o individuale ovvero per la sicurezza dello Stato.

Da ultimo, la norma in esame, prende in considerazione la posizione dell'utilizzatore professionale di sistemi di intelligenza artificiale ad alto rischio, sanzionando l'omessa adozione intenzionale delle necessarie misure di sorveglianza umana, qualora da tale omissione derivi un pericolo per la vita o per l'incolumità pubblica o individuale ovvero per la sicurezza dello Stato.

La *ratio* della disposizione risiede nell'esigenza di estendere la tutela penale anche alle peculiarità dei sistemi di intelligenza artificiale ad alto rischio, superando l'ambito applicativo della tradizionale fattispecie di cui all'art. 437 Cod. Pen., storicamente incentrata sull'omessa predisposizione o rimozione di dispositivi e apparecchiature destinati alla prevenzione di infortuni e disastri.

• ***Illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale (art. 612-quater Cod. Pen.)***

L'art. 612-quater c.p. disciplina la fattispecie concernente l'illecita diffusione di contenuti generati o alterati mediante sistemi di intelligenza artificiale.

La disposizione sanziona la condotta di chi, senza il consenso della persona interessata, diffonda immagini, video o voci falsificati o alterati mediante l'impiego di sistemi di intelligenza artificiale, idonei a indurre in errore circa la loro genuinità, qualora dalla diffusione derivi un danno ingiusto alla persona.

La fattispecie non attribuisce, dunque, rilevanza penale alla mera creazione del contenuto artificiale o alterato, richiedendo la ricorrenza di ulteriori elementi costitutivi, tra i quali la diffusione del contenuto in assenza del consenso dell'interessato, la sua

idoneità a trarre in inganno circa la genuinità e, soprattutto, il verificarsi di un danno ingiusto alla persona.

Nell'ambito dell'attività d'impresa, la fattispecie può assumere particolare rilievo con riferimento ai processi nei quali siano impiegati sistemi di intelligenza artificiale idonei a generare o modificare immagini, registrazioni audio, video o altri contenuti suscettibili di rappresentare persone fisiche.

Particolare attenzione dovrà, pertanto, essere prestata ai processi aziendali concernenti la comunicazione istituzionale e commerciale, le attività di marketing e pubblicità, la gestione dei contenuti digitali e dei social media, la produzione audiovisiva, nonché la gestione dei rapporti con dipendenti, collaboratori, consulenti, fornitori e soggetti terzi incaricati della produzione o della diffusione di contenuti per conto dell'ente.

F.3. AREE A RISCHIO

In relazione ai reati e alle condotte criminose sopra esplicitate, le aree ritenute più specificamente a rischio risultano essere, ai fini della presente Parte Speciale "G" del Modello, le seguenti:

1) progettazione, sviluppo e addestramento di sistemi di IA ad alto rischio; in particolare, l'area di rischio in esame riguarda le attività connesse alla progettazione, sviluppo, addestramento, testing, validazione e messa in esercizio di sistemi di IA qualificabili come ad alto rischio, laddove l'ente partecipi direttamente a tali attività o ne affidi lo svolgimento a soggetti terzi;
2) Acquisto, selezione e gestione di sistemi di IA sviluppati da terzi nonché modifica, configurazione, manutenzione e aggiornamento dei sistemi di IA; il rischio, qui, non riguarda soltanto chi sviluppa direttamente il sistema, ma anche l'impresa che decide di adottarlo e utilizzarlo nell'ambito dei propri processi.
3) Utilizzo professionale di sistemi di IA ad alto rischio e supervisione umana; tale area di rischio si concretizza quando l'impresa utilizza professionalmente un sistema di IA

ad alto rischio e attribuisce allo stesso un ruolo significativo nell'assunzione o nell'esecuzione di decisioni.

4) Comunicazione, marketing, pubblicità e gestione dei social media. Il rischio di commissione reato, qui, sorge nel caso in cui l'ente utilizza sistemi di AI generativa per produrre immagini, video, registrazioni vocali, contenuti pubblicitari.

F.4. DESTINATARI DELLA PARTE SPECIALE – PRINCIPI GENERALI DI COMPORTAMENTO E DI ATTUAZIONE

La presente Parte Speciale si riferisce a comportamenti posti in essere da Soggetti in posizione apicale e dipendenti della Società, Consulenti e *Partner*.

Obiettivo della presente Parte Speciale è che tali soggetti, nella misura in cui possano essere coinvolti nello svolgimento di attività nelle Aree a Rischio, si attengano a regole di condotta conformi a quanto prescritto dalla stessa al fine di prevenire ed impedire il verificarsi dei reati **commessi con l'uso di sistemi di intelligenza artificiale**, pur tenendo conto della diversa posizione di ciascuno dei soggetti stessi nei confronti della Società e, quindi, della diversità dei loro obblighi come specificati nel Modello.

In particolare, la presente Parte Speciale ha la funzione di fornire un elenco dei principi generali e dei principi procedurali specifici cui i Soggetti in posizione apicale e dipendenti della Società, i Consulenti, i Collaboratori e *Partner* in relazione al tipo di rapporto in essere con la Società, sono tenuti ad attenersi ai fini di una corretta applicazione del Modello.

Nell'espletamento di tutte le operazioni attinenti alla gestione sociale, oltre alle regole di cui al presente Modello, i Soggetti in posizione apicale e dipendenti della Società – con riferimento alla rispettiva attività – devono, in generale, conoscere e rispettare tutte le regole, procedure e principi – i quali devono esser intesi come attuativi ed integrativi del Modello – contenuti nei seguenti documenti, le cui modalità di approvazione e modifica rimangono quelle attualmente in vigore:

- il Codice Etico;
- le regole di *corporate governance;*
- individuazione dei requisiti di sicurezza del sistema;
- implementare le misure tecniche necessarie a prevenire malfunzionamenti o alterazioni;
- adottare procedure di monitoraggio del sistema;
- monitorare eventuali alterazioni non autorizzata dei parametri, dei modelli o degli elementi funzionali del sistema;
- selezionare e qualificare i fornitori;
- verificare le caratteristiche e la classificazione del sistema;
- verificare le misure di sicurezza implementate;
- definire le responsabilità tra azienda e fornitore;
- gestire gli aggiornamenti e le modifiche del sistema;
- individuare i soggetti responsabili della supervisione;
- definire le modalità di intervento umano;
- gestire gli errori e gli alert;
- formare gli utilizzatori;
- tracciare gli interventi umani;
- aggiornare il sistema;
- verificare la provenienza del materiale;
- verificare l'eventuale presenza di persone identificabili;
- acquisire, ove necessario, il relativo consenso;
- sottoporre il contenuto a verifica prima della pubblicazione;
- individuare chiaramente i soggetti autorizzati alla diffusione;
- assicurare la tracciabilità dell'approvazione.

F.4. ISTRUZIONI E VERIFICHE DELL'ORGANISMO DI VIGILANZA

I compiti di vigilanza dell'OdV in relazione all'osservanza del Modello per quanto concerne i Reati commessi con l'uso di sistemi di intelligenza artificiale sono i seguenti:

A) verificare l'adeguatezza del sistema dei controlli interni predisposto dall'Ente con riferimento ai processi aziendali che prevedono la progettazione, lo sviluppo, l'acquisizione, l'implementazione, l'utilizzo, la modifica, la manutenzione e l'aggiornamento di sistemi di intelligenza artificiale;

B) vigilare sull'effettiva attuazione dei protocolli e delle procedure aziendali adottati dall'Ente al fine di prevenire la commissione dei reati di cui agli artt. 437-bis e 612-quater Cod. Pen.;

C) verificare che siano adeguatamente individuati e formalizzati i ruoli e le responsabilità dei soggetti coinvolti nei processi di selezione, acquisizione, sviluppo, gestione e utilizzo dei sistemi di intelligenza artificiale, con particolare riguardo ai soggetti cui siano attribuiti compiti di supervisione e controllo dei sistemi di IA ad alto rischio;

D) verificare l'adeguatezza dei flussi informativi verso l'Organismo di Vigilanza, assicurandosi che siano tempestivamente comunicati gli eventi, le anomalie e gli incidenti rilevanti concernenti i sistemi di intelligenza artificiale, nonché le eventuali violazioni delle procedure interne, gli accessi o gli interventi non autorizzati, le modifiche non approvate e ogni altra circostanza potenzialmente rilevante ai fini del D.Lgs. n. 231/2001;

E) vigilare sui processi aziendali concernenti la produzione, approvazione e diffusione di contenuti generati o modificati mediante sistemi di intelligenza artificiale, con particolare riferimento a immagini, video e registrazioni vocali riconducibili a persone fisiche, verificando l'esistenza di adeguati presidi autorizzativi e di controllo, anche con riferimento alla verifica dei consensi e alla legittimità della successiva diffusione.