BonelliErede

Practice Legal Risk, Compliance & Investigations
Focus Team Innovazione e Trasformazione digitale
02 Novembre 2026

Intelligenza artificiale e responsabilità da reato degli enti: il D.Lgs. 160/2026 e l'ampliamento del catalogo dei reati presupposto

Autori

Alessandro De Nicola
alessandro.denicola@belex.com
Tel. +39 02 771131

Tommaso Faelli
tommaso.faelli@belex.com
Tel. +39 02 771131

Marco Dell'Antonia
marco.dellantonia@belex.com
Tel. +39 02 771131

Marco Giovanni Mancino
marco.mancino@belex.com
Tel. +39 02 771131

Riccardo Caselle
riccardo.caselle@belex.com
Tel. +39 02 771131

Jacopo Taddei
jacopo.taddei@belex.com
Tel. +39 02 771131

Miriana Fierro
miriana.fierro@belex.com
Tel. +39 02 771131

Megi Trashaj
megi.trashaj@belex.com
Tel. +39 02 771131

Focus Team Innovazione e Trasformazione Digitale

Focus Team Leader
Tommaso Faelli
tommaso.faelli@belex.com
Tel. +39 02 771131

1. Introduzione

Il 15 settembre 2026 è stato pubblicato in Gazzetta Ufficiale (Serie Generale, n. 214) il **Decreto legislativo 9 settembre 2026, n. 160**[1] ("**D.Lgs. 160**"), in vigore dal **30 settembre 2026**.

La novella detta disposizioni in materia di responsabilità civile e penale connesse all'impiego dell'*Artificial intelligence* ("**AI**"), nonché relative all'utilizzo dei sistemi di AI per l'attività di polizia. Sul piano della responsabilità degli enti da reato, l'intervento normativo determina un'estensione dell'area del rischio *ex* D.Lgs. 8 giugno 2001, n. 231 ("**D.Lgs. 231**") mediante l'ampliamento del catalogo dei cc.dd. reati presupposto.

2. L'art. 25-*vicies* D.Lgs. 231/2001

L'art. 15 del D.Lgs. 160 interviene sulla disciplina della responsabilità amministrativa degli enti di cui al D.Lgs. 231 ampliando il catalogo dei reati presupposto con **due fattispecie** connesse all'utilizzo dei sistemi di intelligenza artificiale.

[1] Recante "*Adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale, in materia di utilizzo dei sistemi di intelligenza artificiale per l'attività di polizia e di responsabilità civile e penale*".

This document is provided as a service to clients and other friends for educational purposes only. It should not be construed or relied on as legal advice or to create a lawyer-client relationship.

In particolare, il nuovo **art. 25-*vicies*** D.Lgs. 231 (*Reati commessi con l'uso di sistemi di intelligenza artificiale*) disciplina la responsabilità da reato dell'ente per la commissione dei seguenti delitti:

- *omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale e alterazione illecita dei sistemi* (**art. 437-*bis* c.p.**)[2];

- *illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale* (**art. 612-*quater* c.p.**)[3].

Sul piano sanzionatorio, nell'ipotesi di responsabilità *ex* art. 25-*vicies* D.Lgs. 231, sono previste a carico dell'ente sia sanzioni **pecuniarie** sia sanzioni **interdittive**.

Con riferimento alle **sanzioni pecuniarie** è prevista l'applicabilità:

- nell'ipotesi di responsabilità per il delitto di cui all'**art. 437-*bis* c.p.**, della sanzione pecuniaria **da euro 154.800** a **euro 1.549.000** (da seicento a mille quote);

- nell'ipotesi di responsabilità per il delitto di cui all'**art. 612-*quater* c.p.**, della sanzione pecuniaria da **euro 51.600** a **euro 1.084.300** (da duecento a settecento quote).

Quanto alle **sanzioni interdittive**, trovano applicazione (tanto nel caso dell'art. 437-*bis* c.p. quanto nell'ipotesi di cui all'art. 612-*quater* c.p.):

- la **sospensione** o la **revoca** delle **autorizzazioni**, **licenze** o **concessioni** funzionali alla commissione dell'illecito;

- il **divieto di contrattare con la pubblica amministrazione**, salvo che per ottenere le prestazioni di un pubblico servizio;

- l'**esclusione** da **agevolazioni**, **finanziamenti**, **contributi o sussidi** e l'eventuale **revoca** di quelli già concessi;

- il **divieto di pubblicizzare beni o servizi**.

---

[2] Fattispecie introdotta nel Codice penale dall'art. 12 del D.Lgs. 160.
[3] Fattispecie introdotta nel Codice penale dall'art. 26 della Legge 23 settembre 2025, n. 132 (*Disposizioni e deleghe al Governo in materia di intelligenza artificiale*).

This document is provided as a service to clients and other friends for educational purposes only.
It should not be construed or relied on as legal advice or to create a lawyer-client relationship.

3. Omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale e alterazione illecita dei sistemi (art. 437-*bis* c.p.)

Il nuovo reato di *Omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale e alterazione illecita dei sistemi*, disciplinato dall'art. 437-*bis* c.p. tra i *Delitti contro l'incolumità pubblica*, si articola in una pluralità di fattispecie di natura sia omissiva che attiva.

Sul versante delle **condotte omissive** è punito:

- con la reclusione da uno a cinque anni, chiunque **ometta di adottare le misure tecniche di sicurezza** previste per "*la progettazione*", "*l'addestramento*", "*la produzione*" e "l'*immissione sul mercato*"[4] di sistemi di AI ad alto rischio, idonee a prevenire malfunzionamenti o alterazioni del funzionamento, ovvero **ometta di adottare misure di sorveglianza umana,** quando da tali omissioni derivi un pericolo per la vita o l'incolumità pubblica o individuale. È prevista la pena della reclusione da due a otto anni qualora dal fatto derivi un pericolo per la sicurezza dello Stato (art. 437-*bis*, comma 1, c.p.). Tali condotte sono punite anche se realizzate con **colpa grave**, con una riduzione delle cornici edittali da un terzo a un sesto (art. 437-*bis*, comma 3, c.p.);

- con le stesse pene di cui al comma 1 (e richiamate nel punto precedente) l'utilizzatore professionale di sistemi di AI ad alto rischio che **ometta "*intenzionalmente*" di adottare le misure di sorveglianza umana** (art. 437-*bis*, comma 4, c.p.)[5].

[4] Pur essendo il delitto in commento costituito come fattispecie di reato comune che può essere realizzata da *"chiunque"*, il riferimento alle attività di *"progettazione"*, *"addestramento"*, *"produzione"* e *"immissione sul mercato"* circoscrive, di fatto, la platea dei soggetti attivi della fattispecie alla filiera professionale dell'AI, escludendo in concreto l'utilizzatore finale.

[5] Si segnala che il testo definitivo della novella in analisi presenta una differenza significativa rispetto allo schema di Decreto Legislativo trasmesso alle Camere prima dell'approvazione del D.Lgs. 160. L'utilizzo professionale del sistema ad alto rischio, che nello schema figurava tra le attività disciplinate dal primo comma, è stato successivamente isolato nel quarto comma, con una limitazione di responsabilità penale per l'utilizzatore professionale alla sola omissione delle misure di sorveglianza, omissione punibile soltanto se commessa intenzionalmente dal soggetto attivo. Il testo finale del D.Lgs. 160 esclude anche che all'utilizzatore professionale sia estesa la disposizione in materia di responsabilità per colpa grave.

This document is provided as a service to clients and other friends for educational purposes only.
It should not be construed or relied on as legal advice or to create a lawyer-client relationship.

Con riferimento alle **condotte attive** è punito:

- con la reclusione da due a sei anni, in via residuale (cioè salvo che il fatto costituisca più grave reato e al di fuori delle ipotesi sopra descritte), chiunque **alteri sistemi** di AI ad alto rischio, quando dal fatto derivi un pericolo per la vita o l'incolumità pubblica o individuale. È prevista la pena da tre a dieci anni qualora dal fatto derivi un pericolo per la sicurezza dello Stato (art. 437-*bis*, comma 2, c.p.).

Le diverse ipotesi disciplinate dall'art. 437-*bis* c.p., sono configurate come fattispecie di **pericolo concreto** (applicabili, per esempio, in caso di pericolo per "*la vita*" o "*l'incolumità*" pubblica o individuale).

3.1 I sistemi di intelligenza artificiale ad alto rischio

Le condotte descritte dall'art. 437-*bis* c.p. sono accomunate dall'oggetto sul quale ricade la condotta di reato, cioè il "***sistema di intelligenza artificiale** ad **alto rischio***": si tratta di una nozione che non si rinviene nella fattispecie penale, ma che va ricostruita alla luce delle definizioni richiamate dall'art. 11 del D.Lgs. 160, il quale rinvia all'art. 3 del Reg. (UE) 2024/1689 ("**AI Act**" o "**Regolamento**").

L'art. 3, n. 1, dell'AI Act definisce "***sistema di AI***" un "*sistema automatizzato progettato per funzionare con livelli di autonomia variabili*" e che "*deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali*".

L'art. 6 del Regolamento detta specifiche regole di classificazione e impone di considerare "***ad alto rischio***" due macro-categorie di sistemi di intelligenza artificiale, come si dirà meglio nei prossimi paragrafi[6].

---

[6] Si segnala che, nonostante il D.Lgs. 160, come anticipato, abbia come data di entrata in vigore il 30 settembre 2026, le disposizioni dell'AI Act (che verranno richiamate nei prossimi paragrafi quali elementi di interpretazione sistematica per le disposizioni penali) presenti nel Capo III del Regolamento in questione *(Sistemi di IA ad alto rischio), Sezione I (Classificazione dei sistemi di AI come "ad alto rischio"),* Sezione II *(Requisiti per i sistemi di IA ad alto rischio),* Sezione III *(Obblighi dei fornitori e dei deployer dei sistemi di IA ad alto rischio e di altre parti*), che contengono gli artt. da 6 a 27 dell'AI Act, sezioni 1-3, del Regolamento, entreranno in vigore dal **2 agosto 2028** per i sistemi ad alto rischio dell'Allegato I e dal **2 dicembre 2027** per quelli dell'Allegato III (art. 113 AI Act), per effetto del Reg. (UE) 2026/1744 (c.d. ***Digital Omnibus***).

This document is provided as a service to clients and other friends for educational purposes only.
It should not be construed or relied on as legal advice or to create a lawyer-client relationship.

3.1.1 Sistemi di AI quali componenti di sicurezza o prodotti (Allegato I)

È considerato ad alto rischio il **sistema di AI che è componente di sicurezza**[7] dei prodotti o che è esso stesso prodotto qualora (congiuntamente):

- esso ricada nella disciplina di una delle norme elencate nell'**Allegato I dell'AI Act**[8] (art. 6, par. 1, lett. a, AI Act);

- esso sia soggetto, ai sensi della medesima normativa elencata nell'Allegato I, **a una valutazione della conformità da parte di terzi** ai fini dell'immissione sul mercato o della messa in servizio (art. 6, par. 1, lett. b, AI Act)[9].

L'Allegato I, che quindi costituisce punto di riferimento per identificare i sistemi AI ad alto rischio che rientrano nella categoria descritta, contiene un lungo elenco di norme UE ove sono ricomprese le regole riguardanti, a titolo esemplificativo, *giocattoli*, *ascensori*, *apparecchi utilizzati in atmosfera potenzialmente esplosiva*, *apparecchiature radio*, *attrezzature a pressione*, *imbarcazioni da diporto e moto d'acqua*, *impianti a fune*, *apparecchi che bruciano carburanti gassosi*, *dispositivi medici*, *dispositivi medico-diagnostici in vitro*, *prodotti macchina*, *veicoli automobilistici*, *equipaggiamento marittimo*[10].

---

[7] Il considerando 7 del Digital Omnibus prevede che la nozione di "componente di sicurezza" dovrebbe essere "***circoscritta in modo da includere unicamente i sistemi di IA che potrebbero incidere negativamente sulla salute e sulla sicurezza delle persone o dei beni****, in linea con* ***l'approccio basato sul rischio*** *di tale regolamento*" e che "*la funzione di sicurezza dovrebbe essere* ***una finalità prevista del sistema, determinata dal fornitore del sistema stesso***". L'art. 3, n. 14 dell'AI Act è stato dunque modificato dal Digital Omnibus come segue: "*un componente di un prodotto o di un sistema di IA che svolge una funzione di sicurezza per tale prodotto o sistema di IA o il cui guasto o malfunzionamento mette in pericolo la salute e la sicurezza di persone o beni;* ***ai fini della presente definizione, un componente svolge una funzione di sicurezza se la sua finalità prevista è prevenire o attenuare i rischi per la salute e la sicurezza di persone o beni***".

[8] Contenente *Elenco della normativa di armonizzazione dell'Unione*.

[9] Oltre al testo normativo richiamato, in via interpretativa sul punto rileva il considerando n. 50 dell'AI Act*: "per quanto riguarda i sistemi di AI che sono componenti di sicurezza di prodotti, o che sono essi stessi prodotti, e rientrano nell'ambito di applicazione di una determinata normativa di armonizzazione dell'Unione elencata nell'allegato al presente regolamento, è opportuno classificarli come sistemi ad alto rischio a norma del presente regolamento se il prodotto interessato è sottoposto alla procedura di valutazione della conformità con un organismo terzo di valutazione della conformità a norma della suddetta pertinente normativa di armonizzazione dell'Unione*".

[10] Come precisato dal Digital Omnibus mediante l'introduzione dei nuovi paragrafi 1-*bis*, 1-*ter* e 1-*quater* dell'art. 6 dell'AI Act, è escluso che ricadano nell'ambito della definizione di sistemi di AI ad alto rischio i sistemi utilizzati **esclusivamente** per assistenza agli utenti, ottimizzazione delle prestazioni, efficienza dei servizi, automazione o praticità o controllo della qualità (art. 6, par. 1-*bis*, AI Act), a meno che il guasto o malfunzionamento possa mettere a rischio la salute e la sicurezza (art. 6, par. 1-*ter*, AI Act). Una disposizione particolare è dettata con riferimento ai prodotti che presentano rischi relativi alla

This document is provided as a service to clients and other friends for educational purposes only.
It should not be construed or relied on as legal advice or to create a lawyer-client relationship.

3.1.2 Sistemi di AI ad alto rischio c.d. indipendenti (Allegato III)

Come anticipato, oltre a quelli finora descritti, vi sono poi i **sistemi di AI ad alto rischio c.d. indipendenti** (art. 6, par. 2, AI Act), la cui individuazione in concreto passa per l'elencazione effettuata dal legislatore europeo nell'**Allegato III** dell'AI Act[11]. In questo caso l'enumerazione procede per settori. Sono ricompresi nell'Allegato III:

- **la biometria**;
- **le infrastrutture critiche**;
- **l'istruzione e la formazione professionale**;
- **l'occupazione, la gestione dei lavoratori e l'accesso al lavoro autonomo**;
- **l'accesso e fruizione dei servizi pubblici e privati essenziali**;
- **le attività di contrasto delle agenzie di controllo**;
- **migrazione, asilo e la gestione del controllo delle frontiere**;
- **l'amministrazione della giustizia e i processi democratici**.

La riconducibilità a un caso d'uso dell'Allegato III non determina automaticamente la classificazione del sistema di AI come ad alto rischio. L'art. 6, par. 3, infatti, **esclude** la classificazione di alto rischio per quei sistemi AI che, pur rientrando in una delle ipotesi previste dall'Allegato III, **non** presentino un rischio significativo di danno per la salute, la sicurezza **o i diritti fondamentali delle persone fisiche**.

---

distribuzione dello spettro radio o alle interferenze elettromagnetiche che non incidono sulla salute e sulla sicurezza (art. 6, par. 1-*quater*, AI Act).

[11] Come illustrato dal considerando n. 52 dell'AI Act: "*I sistemi di AI* ***indipendenti*** [...] sono *utilizzati in una serie di* ***settori*** *specificamente predefiniti indicati nel presente regolamento*". L'art. 7 dell'AI Act conferisce alla Commissione il potere di adottare atti delegati al fine di modificare l'Allegato III aggiungendo o modificando i casi d'uso dei sistemi di AI ad alto rischio (disposizione finalizzata a "*tenere conto del rapido ritmo dello sviluppo tecnologico nonché dei potenziali cambiamenti nell'uso dei sistemi di AI*", considerando n. 52).

This document is provided as a service to clients and other friends for educational purposes only.
It should not be construed or relied on as legal advice or to create a lawyer-client relationship.

3.2 Misure tecniche di sicurezza e di sorveglianza umana

La condotta omissiva descritta dall'art. 437-*bis* c.p. consiste, come anticipato, nella mancata adozione di:

- "***misure tecniche di sicurezza*** [...] ***idonee a prevenire malfunzionamenti o alterazioni del funzionamento***";

- "***misure di sorveglianza umana***".

Le formule adottate sono elastiche e il legislatore nazionale non fornisce un decalogo di quali siano le misure tecniche e di sorveglianza umana la cui omissione può costituire illecito penalmente rilevante. Di conseguenza anche con riferimento a tale aspetto, per evitare ipotesi di **colpa di organizzazione**, si rende indispensabile guardare alla normativa di riferimento in materia di AI.

3.2.1 Misure tecniche di sicurezza

Con riferimento alle misure tecniche di sicurezza idonee a prevenire malfunzionamenti o alterazioni del funzionamento di sistemi AI ad alto rischio, l'AI Act, come noto, impone, nei confronti di diverse categorie di soggetti, molteplici obblighi. Tra i principali si segnalano i seguenti:

- l'obbligo per il fornitore[12] di **istituire, attuare, documentare e mantenere un "*sistema di gestione dei rischi*"** (artt. 9 e 17, AI Act);

- l'obbligo per gli importatori di **verificare che il fornitore del sistema abbia eseguito la procedura di valutazione** della conformità (art. 23 AI Act);

---

[12] Si noti che i soggetti di cui alle definizioni dell'AI Act non coincidono perfettamente con le attività elencate dal legislatore italiano nel testo dell'art. *437-bis* c.p., dove, per esempio, non è utilizzato il termine "*fornitura*" ma "*progettazione*", "*produzione*" e "*immissione sul mercato*". Queste ultime attività (che, stando alla norma italiana in commento, individuano le regole di condotta di settore che potrebbero dar luogo a responsabilità qualora omesse) ricadrebbero comunque nelle attività proprie del "***fornitore***" per come definito dall'AI Act che considera tale "*una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che sviluppa un sistema di AI o un modello di AI per finalità generali o che fa sviluppare un sistema di AI o un modello di AI per finalità generali e immette tale sistema o modello sul mercato o mette in servizio il sistema di AI con il proprio nome o marchio, a titolo oneroso o gratuito*" (art. 3, par. 1, n. 3, AI Act).

This document is provided as a service to clients and other friends for educational purposes only.
It should not be construed or relied on as legal advice or to create a lawyer-client relationship.

- l'obbligo per i *deployer*[13] di **utilizzare i sistemi conformemente alle istruzioni per l'uso che accompagnano i sistemi** (art. 26 AI Act).

Nella definizione della condotta doverosa rilevante ai fini dell'art. 437-*bis* c.p. assumono rilievo centrale anche i cc.dd. **standard tecnici armonizzati**.

L'art. 40, par. 1, dell'AI Act **prevede una presunzione di conformità** ad alcuni requisiti del Regolamento per i sistemi di AI ad alto rischio conformi agli standard armonizzati i cui riferimenti siano stati pubblicati nella Gazzetta ufficiale dell'Unione europea.

La Commissione europea ha richiesto agli enti di normalizzazione l'elaborazione degli standard destinati a supportare l'attuazione dell'AI Act. Su questo fronte, si segnala che nel luglio 2026 è stato pubblicato **EN 18286:2026** (***Artificial intelligence – Quality management system for EU AI Act regulatory purposes***) e il 14 ottobre 2026 è stata pubblicata la relativa *Decisione di esecuzione 2026/2274 della Commissione del 12 ottobre 2026 relativa alle norme armonizzate per i sistemi di IA ad alto rischio redatte a sostegno del regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio*, mentre è in elaborazione prEN 18228 (*Practical Risk Management System Requirements for AI*) dedicato all'AI Risk Management e destinato a supportare l'applicazione dell'art. 9 del Regolamento.

3.2.2 Sorveglianza umana

L'altra condotta che rileva penalmente ai fini dell'art. 437-*bis* c.p. è quella relativa all'omissione di "**misure di sorveglianza umana**".

In questo caso il riferimento normativo è contenuto all'**art. 14** dell'AI Act, il quale richiede che **i sistemi ad alto rischio siano progettati e sviluppati**, anche con strumenti di interfaccia uomo-macchina, "***in modo tale da poter essere efficacemente supervisionati da persone fisiche*** *durante il periodo in cui sono in uso*" (art. 14, par. 1, AI Act).

---

[13] Il "***deployer***" è *"una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che* ***utilizza*** *un sistema di AI sotto la propria autorità, tranne nel caso in cui il sistema di AI sia utilizzato nel corso di un'attività personale non professionale*" (art. 3, par. 1, n. 4, AI Act).

This document is provided as a service to clients and other friends for educational purposes only.
It should not be construed or relied on as legal advice or to create a lawyer-client relationship.

Le misure di sorveglianza umana – che comunque devono essere commisurate ai "*rischi*", *"al livello di autonomia*" e "*al contesto di utilizzo*" del sistema di AI ad alto rischio – sono attuate con:

- **misure individuate e integrate nel sistema dal fornitore** (prima della immissione sul mercato o della messa a disposizione);

  oppure:

- **misure**, individuate dal fornitore, ma **attuate dal *deployer*** (art. 14, par. 3, AI Act).

Sul piano operativo, la normativa europea richiede che le persone fisiche cui è affidata la sorveglianza umana siano poste nelle condizioni, *inter alia*, di: (i) comprendere capacità e limiti del sistema e di monitorarne il funzionamento, individuando anomalie, disfunzioni o prestazioni inattese; (ii) interpretarne correttamente i risultati; (iii) infine, di intervenire direttamente sul funzionamento del sistema o di interromperlo attraverso un «*pulsante di "arresto"*» o una procedura analoga (art. 14, par. 4, AI Act)[14].

È inoltre previsto l'obbligo per il *deployer* di **affidare la sorveglianza umana a persone fisiche dotate della necessaria** "*competenza*", "*formazione*", "*autorità*", nonché di "*un adeguato sostegno*" (art. 26, par. 2, AI Act).

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

L'**art. 612-*quater* c.p.** in materia di *Illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale* era stato introdotto nel catalogo dei reati presupposto con la Legge 23 settembre 2025, n. 132[15]. Il delitto ha la finalità di contrastare il fenomeno del c.d. ***deep fake***[16].

La fattispecie punisce, con la reclusione da uno a cinque anni, chiunque cagioni 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.

---

[14] Una particolare **forma di sorveglianza umana rafforzata** è prevista dal par. 5 relativamente ad alcuni sistemi biometrici ad alto rischio (lett. a), punto 1, Allegato III, AI Act).

[15] Al commento della Legge era stata dedicata una **precedente** *newsletter*, alla quale si rinvia, disponibile su questo sito.

[16] Definito dall'art. 3, n. 60, AI Act come "*un'immagine o un contenuto audio o video generato o manipolato dall'AI che assomiglia a persone, oggetti, luoghi, entità o eventi esistenti e che apparirebbe falsamente autentico o veritiero a una perso*na".

This document is provided as a service to clients and other friends for educational purposes only.
It should not be construed or relied on as legal advice or to create a lawyer-client relationship.

Il delitto è procedibile a querela della persona offesa, salvo che il fatto sia connesso con altro delitto procedibile d'ufficio, ovvero sia commesso nei confronti di persona incapace, per età o infermità, o di una pubblica autorità a causa delle funzioni esercitate.

5. Conclusioni

L'inserimento dei reati in materia di AI nel catalogo dei reati presupposto richiede che le società procedano sin d'ora con l'adeguamento dei Modelli 231 e la strutturazione di una *governance* aziendale in linea con i nuovi obblighi normativi.

In questa prospettiva, tra i principali interventi da valutare rientrano:

- la **mappatura e** la **classificazione** dei sistemi di intelligenza artificiale prodotti, sviluppati, addestrati, immessi sul mercato o utilizzati dall'ente;

- lo svolgimento di uno **specifico *risk assessment*** volto a individuare i processi e le attività maggiormente esposti ai nuovi rischi;

- la **revisione e** l'**aggiornamento del Modello 231**, che tenga conto dei nuovi rischi individuati, e del sistema normativo interno ed europeo, mediante l'introduzione di princìpi e presìdi specificamente dedicati all'utilizzo dei sistemi di intelligenza artificiale;

- l'**integrazione del Codice Etico** con princìpi in materia di uso responsabile dell'AI;

- la chiara **individuazione dei soggetti** autorizzati all'utilizzo dei sistemi AI e, nel caso di sistemi di intelligenza artificiale ad alto rischio, delle persone fisiche incaricate della sorveglianza umana;

- l'erogazione di **specifiche attività formative** al *top management* e ai dipendenti, con la previsione di moduli specifici per il personale addetto alla sorveglianza umana.

This document is provided as a service to clients and other friends for educational purposes only.
It should not be construed or relied on as legal advice or to create a lawyer-client relationship.

Practice Legal Risk, Compliance & Investigations

Alessandro De Nicola

Marco Dell'Antonia

Vincenzo Dell'Osso

Marco Giovanni Mancino

Laura Cappiello

Focus Team Innovazione e Trasformazione digitale

Il *Focus Team* è una costellazione di competenze in diversi ambiti di attività con *focus* su innovazione e trasformazione digitale.

Tommaso Faelli
IP-IT-Privacy

Marco Adda
Tax

Giulia Bianchi Frangipane
Corporate

Enrico Chieppa
Litigation & Dispute Resolution

Gianpaolo Ciervo
Banking

Alessandro De Nicola
Legal Risk, Compliance & Investigations

Vittorio Pomarici
Labour law

Fabrizio Colonna
Financial Regulatory

Maurizio Pappalardo
Antitrust

Matteo Viani
Tax

Luca Guerrini
Litigation & Dispute Resolution

Anna La Mura
Privacy-Data Protection

Giulia Tenaglia
IP-IT-Privacy

This document is provided as a service to clients and other friends for educational purposes only.
It should not be construed or relied on as legal advice or to create a lawyer-client relationship.