Notiziario Sicurezza & Privacy

Aggiornamenti, linee guida e approfondimenti tecnici per imprese e professionisti

SicurBook®

E.L.S.A.
Esperti Lavoro Sicuro Ascom
CONFCOMMERCIO

N°	Mese	Anno
08	Settembre	2026

Scansiona QR code per visitare il nostro sito
www.scssicurezza.it



INTELLIGENZA ARTIFICIALE E RESPONSABILITÀ PENALE: LE NOVITÀ INTRODOTTE DAL D.lgs. n. 160/2026

Il **D.lgs. 9 settembre 2026, n. 160**, pubblicato nella Gazzetta Ufficiale n. 214 del 15 settembre 2026 ed in vigore dal **30 settembre 2026**, interviene sulla disciplina della responsabilità civile e penale connessa all'utilizzo dei sistemi di intelligenza artificiale, in attuazione della legge n. 132/2025 e nel quadro del Regolamento (UE) 2024/1689 – AI Act.

Per imprese e professionisti, le principali novità riguardano l'introduzione del nuovo **art. 437-bis c.p.**, dedicato alla sicurezza dei sistemi di IA ad alto rischio, e l'ampliamento del catalogo dei reati presupposto del **D.lgs. n. 231/2001**, attraverso il nuovo art. 25-vicies.

Novità	Contenuto
Nuovo art. 437-bis c.p.	Introduzione del delitto di omessa adozione delle misure di sicurezza e di sorveglianza umana e di alterazione illecita dei sistemi di IA ad alto rischio.
Nuovo art. 25-vicies D.lgs. n. 231/2001	Inserimento tra i reati presupposto dell'art. 437-bis c.p. e dell'art. 612-quater c.p., relativo alla diffusione illecita di contenuti generati o alterati mediante IA.

Il nuovo art. 437-bis c.p.

La principale novità sul piano penale è rappresentata dall'introduzione dell'**art. 437-bis c.p.**, rubricato *"**Omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale e alterazione illecita dei sistemi**"*, collocato successivamente all'art. 437 c.p. ("Rimozione od omissione dolosa di cautele contro infortuni sul lavoro").

La norma prevede:

***«c.1**: **Chiunque omette di adottare le misure tecniche di sicurezza, previste per la progettazione, l'addestramento, la produzione, l'immissione sul mercato di sistemi di intelligenza artificiale ad alto rischio, idonee a prevenire malfunzionamenti o alterazioni del funzionamento dei sistemi** ovvero **omette di adottare misure di sorveglianza umana** è punito con la **reclusione da uno a cinque anni**, quando da tali omissioni derivi pericolo per la vita o l'incolumità pubblica o individuale.*

*Qualora dal fatto derivi un **pericolo per la sicurezza dello Stato**, la pena è della **reclusione da due a otto anni.***

***c.2**: Salvo che il fatto costituisca più grave reato, **chiunque**, al di fuori dei casi indicati al primo comma, **altera sistemi di intelligenza artificiale ad alto rischio è punito, qualora dal fatto derivi un pericolo per la vita o l'incolumità pubblica o individuale**, con la **reclusione da due a sei anni**. Qualora dal fatto derivi un pericolo per la **sicurezza dello Stato**, la pena è della reclusione **da tre a dieci anni**.*

***c.3**: Se taluno dei fatti previsti dal comma primo è commesso per colpa grave, la pena è ridotta da un terzo a un sesto.*

c.4**: **L'utilizzatore professionale di sistemi di intelligenza artificiale ad alto rischio** che **omette intenzionalmente di adottare misure di sorveglianza umana** è punito con le pene previste dal primo comma, primo e secondo periodo, **qualora da tale omissione derivi, rispettivamente, pericolo per la vita o l'incolumità pubblica o individuale oppure un pericolo per la sicurezza dello Stato.»

In particolar modo, l'art. 437 bis c.p. riguarda specificamente i sistemi di IA ad alto rischio (art. 6 AI act) e pone maggior attenzione sia alle misure tecniche di sicurezza, sia alla sorveglianza umana.

Si tratta di fattispecie di **pericolo concreto**: in tal senso, la mera inosservanza della misura non è sufficiente, in quanto è necessario che dalla condotta derivi un effettivo pericolo per la vita o l'incolumità pubblica o individuale oppure per la sicurezza dello Stato.

⚠ Condotta	Pericolo per la vita / incolumità	Pericolo per la sicurezza dello Stato
Omessa adozione di misure di sicurezza o di sorveglianza umana	Reclusione da 1 a 5 anni	Reclusione da 2 a 8 anni
Stesse omissioni commesse con colpa grave	Pena ridotta da un terzo a un sesto	Pena ridotta da un terzo a un sesto
Alterazione di sistemi di IA ad alto rischio	Reclusione da 2 a 6 anni	Reclusione da 3 a 10 anni
Omissione intenzionale della sorveglianza umana da parte dell'utilizzatore professionale	Reclusione da 1 a 5 anni	Reclusione da 2 a 8 anni

Inoltre, l'ambito di applicazione della norma si rivolge anche alla posizione dell'**utilizzatore professionale**, ossia chi utilizza un sistema di IA ad alto rischio nell'ambito della propria attività può assumere rilievo penale qualora ometta intenzionalmente le previste misure di sorveglianza umana e da tale omissione derivi il pericolo richiesto dalla norma.
Infine, è prevista altresì una specifica forma di responsabilità per **colpa grave** con riferimento alle omissioni contemplate dal primo comma.

Intelligenza artificiale e responsabilità degli enti ex. D.lgs. n. 231/2001: i nuovi reati presupposto

Il D.lgs. n. 160/2026 interviene anche sul tema della responsabilità penale-amministrativa prevista dal **D.lgs. n. 231/2001**, introducendo il nuovo **art. 25-vicies**, rubricato *"**Reati commessi con l'uso di sistemi di intelligenza artificiale**"*.
Pertanto, entrano nel catalogo dei reati presupposto il nuovo **art. 437-bis c.p.** e l'**art. 612-quater c.p.**, relativo all'illecita diffusione di contenuti generati o alterati mediante sistemi di intelligenza artificiale.
In particolare, si segnala che, seppur quest'ultima fattispecie era già stata introdotta dalla **legge n. 132/2025**, il D.lgs. n. 160/2026 ha proceduto al suo inserimento tra i reati che possono determinare la responsabilità dell'ente.

L'art. 612-quater c.p. dispone:
«c.1: Chiunque cagiona un danno ingiusto ad 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, è punito con la reclusione da uno a cinque anni.

c.2: Il delitto è punibile a querela della persona offesa. Si procede tuttavia d'ufficio se il fatto è connesso con altro delitto per il quale si deve procedere d'ufficio ovvero se è commesso nei confronti di persona incapace, per età o per infermità, o di una pubblica autorità a causa delle funzioni esercitate.»
*La disposizione riguarda in particolare la diffusione di **deepfake**, ossia "un'immagine o un contenuto audio o video generato o manipolato dall'IA che assomiglia a persone, oggetti, luoghi, entità o eventi esistenti e che apparirebbe falsamente autentico o veritiero a una persona" (art. 3, n.60 AI act).*

Nuovi reati presupposto e sanzioni per l'ente

Reato presupposto	Sanzione pecuniaria	Sanzioni interdittive
Art. 437-bis c.p. – Omessa adozione di misure di sicurezza nei sistemi di IA e alterazione illecita dei sistemi	**da 600 a 1.000 quote**	**Sì**
Art. 612-quater c.p. – Illecita diffusione di contenuti generati o alterati con sistemi di IA	**da 200 a 700 quote**	**Sì**

Inoltre, in entrambe le fattispecie possono trovare applicazione altresì le sanzioni tipiche interdittive previste dall'art. 9, comma 2, lett. b), c), d) ed e), del D.lgs. n. 231/2001: **sospensione o revoca di autorizzazioni, licenze o concessioni**, **divieto di contrattare con la Pubblica Amministrazione**, **esclusione da agevolazioni, finanziamenti, contributi o sussidi** e **divieto di pubblicizzare beni o servizi**.

Cosa cambia per le imprese

Il nuovo quadro rafforza la necessità, per le organizzazioni che sviluppano o utilizzano sistemi di intelligenza artificiale, di adottare una gestione strutturata dei relativi rischi. Se, da un lato, l'impiego dell'intelligenza artificiale può offrire significativi vantaggi in termini di **ricerca, sviluppo e ottimizzazione dei processi aziendali**, dall'altro non possono essere trascurate le possibili implicazioni in materie quali la **privacy e protezione dei dati personali, proprietà industriale e mercati finanziari**.

In tale contesto, anche alla luce dei principi e degli obblighi previsti dall'**AI Act**, **formazione del personale e adeguati sistemi di controllo e supervisione** rappresentano due presidi fondamentali per prevenire e gestire i rischi connessi all'utilizzo dell'IA in azienda.

Inoltre, con specifico riguardo agli enti dotati di **Modello 231**, assume particolare rilievo la verifica dell'adeguatezza del ***risk assessment***, dei protocolli di prevenzione e dei flussi informativi verso l'Organismo di Vigilanza.

Area di intervento	Cosa verificare / fare
Censimento e classificazione dei sistemi di IA	Individuare i sistemi utilizzati, le finalità, i fornitori e le funzioni aziendali coinvolte, verificando la relativa classificazione e l'eventuale qualificazione come sistema di IA ad alto rischio.
Ruoli, responsabilità e sorveglianza umana	Individuare i soggetti che utilizzano e controllano i sistemi, definendo responsabilità e modalità effettive di supervisione umana.
Sicurezza, monitoraggio e tracciabilità	Adottare misure tecniche e organizzative adeguate a prevenire malfunzionamenti, alterazioni o utilizzi impropri e documentare le attività di controllo e monitoraggio.
Modello 231 e presidi interni	Valutare l'aggiornamento del *risk assessment*, dei protocolli di prevenzione e dei flussi verso l'Organismo di Vigilanza alla luce dei nuovi reati presupposto.
Formazione e alfabetizzazione	Garantire una formazione adeguata ai soggetti che utilizzano o supervisionano sistemi di IA, anche in coordinamento con gli obblighi di alfabetizzazione previsti dall'AI Act.

Il D.lgs. n. 160/2026 rafforza quindi il passaggio da un utilizzo non strutturato dell'intelligenza artificiale a una **gestione organizzata, documentata e controllata**, nella quale sicurezza, sorveglianza umana e tracciabilità assumono rilievo anche ai fini della **prevenzione penale e della responsabilità dell'ente**

Spett.le Cliente,
riceve la presente newsletter, sotto forma di **notiziario SICUR BOOK®,** quale informativa specifica in materia di sicurezza sul lavoro e protezione dati personali, in quanto cliente che ha usufruito e/o usufruisce dei nostri servizi in materia di sicurezza sul lavoro e/o protezione dati personali; se non desidera più ricevere il presente notiziario, potrà disdirlo in qualunque momento, inviando una comunicazione via email come quella indicata a fondo pagina.
Se desidera ricevere informazioni in merito sui servizi da noi erogati, o in merito a quanto indicato nel presente notiziario dai propri collaboratori, Le chiediamo cortesemente di compilare il format sotto riportato e inviarlo a info@sicurezzascs.it:

Tipo Richiesta	Informazioni relative a:

Persona che richiede informazioni:

Nome	
Cognome	
Ruolo	
Telefono	
Indirizzo	
Cap	
Città	
Provincia	

Questo documento è inviato esclusivamente per il destinatario. Tutte le informazioni ivi contenute, compresi eventuali allegati, sono soggette a riservatezza a termini del vigente GDPR 679/2016 in materia di protezione dei dati personali e quindi ne è proibita l'utilizzazione. Se avete ricevuto per errore questa newsletter, Vi preghiamo cortesemente di contattare immediatamente il mittente e cancellare la e-mail dandocene immediata comunicazione, utilizzando il fac simile sotto riportato.
Informativa privacy art. 13 Regolamento UE n. 2016/679: Titolare del trattamento dei dati è SCS SICUREZZA SRL UNIPERSONALE con sede Via Sestri, 3/3 – 16154 Genova.
Sito internet www. scssicurezza.it tel. 010.37762.92 - Contitolare Trattamento Roberto Ferro - Contitolare Trattamento CSA Centro Sicurezza Applicata di Alessandro Ferro & C. sas
Per cancellarti dal ricevere le newsletter di SICUR BOOK invia Email a info@sicurezzascs.it unito ad un documento di riconoscimento della persona autorizzata (vedi anche sito Garante della privacy)
Garanzia di riservatezza e tutela della privacy GDPR 679/2016
Per cancellare o modificare gli argomenti di tuo interesse delle newsletter di SICUR BOOK NEWS invia la presente:

☞ **Richiesta Cancellazione invio via email del SICUR BOOK a: info@sicurezzascs.it**

(art. 21, paragrafo 2 del Regolamento (UE) 2016/679)

Il Sottoscritto: _____in qualità di _____
dell'azienda_____
con sede:_____email_____

richiede la cancellazione dell'invio di newsletter quale il notiziario SICUR BOOK con effetto immediato
data___/____/_____ firma avente diritto richiesta

_____

[1]Allegare copia di un documento di riconoscimento

☞ Per informazioni:

SCS SICUREZZA srl Unipersonale	Via Sestri 3/3 Genova tel.010.377.62.92 p.i. 01574270995	info@sicurezzascs.it web:www.scssicurezza.it
C.T.P. Roberto Ferro **Sicurezza sul lavoro - CTP** **DPO - GDPR 679/2016**	Tel:348.31.27.720	ferro@sicurezzascs.it info@sicurezzascs.it

In collaborazione con:

Avv. Tommaso Ferro Consulenza legale e formazione	Tel:347.14.20.113	avvtommasoferro@gmail.com

In collaborazione con:

CSA CENTRO SICUREZZA APPLICATA	Via delle Primule 101 16148 Genova Tel. 010.0899266/345	ufficio@csasicurezza.it
Dott. Alessandro Ferro	Tel:010.0899266/345	ufficio@csasicurezza.it
Dott.ssa Irene Carella	Tel:010.0899266/345	ufficio@csasicurezza.it
Dott. Nicolò Ferro	Tel:010.0899266/345	ufficio@csasicurezza.it

