

Cyber Resilience Act

# Allinea

Avvera Compliance Review

Amazon v. Perplexity

Sanctions Avvera

Avvera alla Scuola Nazionale di Educazione Civica di Palazzo Montecitorio

Frodi con voce clonata

Intelligenza artificiale e responsabilità degli enti

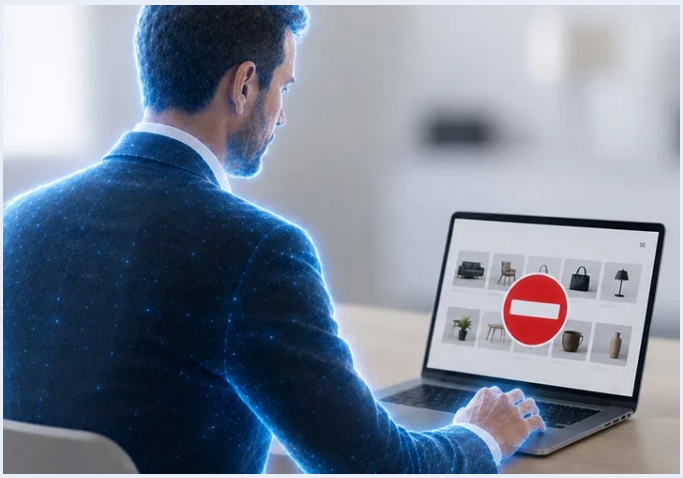
Settembre 2026

Allinea
Avvera Compliance Review
Settembre 2026

# Amazon v. Perplexity

## La Corte d'appello federale attribuisce all'utente la responsabilità dell'agente. E lascia aperto il vero problema.

Con l'opinion del 4 agosto 2026, la US Court of Appeals for the Ninth Circuit ha riformato il provvedimento inibitorio ottenuto in primo grado da Amazon nei confronti di Perplexity, stabilendo che l'accesso ai sistemi del gigante dell'e-commerce era imputabile all'utente finale e non alla società che aveva sviluppato l'agente. Il collegio ha espressamente circoscritto la portata della decisione all'interpretazione del Computer Fraud and Abuse Act federale e del Comprehensive Computer Data Access and Fraud Act californiano. Il ragionamento, tuttavia, offre spunti che oltrepassano il perimetro dichiarato.



**Il funzionamento di Comet e la questione dell'accesso**

Il browser Comet, sviluppato da Perplexity, opera in modalità assistente acquisendo uno screenshot della finestra visualizzata, trasmettendolo ai server della società, che lo analizzano e generano le istruzioni che il browser eseguirà per interagire con il sito di destinazione. L'architettura coinvolge quindi tre elementi: l'assistente, che non opera in autonomia; l'infrastruttura di Perplexity; l'utente, che impartisce le istruzioni. Amazon aveva comunicato a Perplexity di non consentire l'interazione di assistenti automatizzati sul proprio sito. La comunicazione non era stata rispettata. Il collegio ha ritenuto improbabile che Amazon potesse dimostrare un "accesso" di Perplexity ai propri sistemi nel senso richiesto dal CFAA: ad accedere sarebbe stato l'utente, avvalendosi dell'assistente quale mero strumento.

*"L'intelligenza artificiale resta software: complesso quanto si voglia, ma il cui funzionamento è determinato da scelte umane che ne comportano l'assunzione delle conseguenze"*

**Il profilo condivisibile: la responsabilità resta della persona**

Sul piano dei principi, la decisione consolida un assunto che merita di essere sottolineato. Da tempo si assiste alla proposizione di narrative - non disinteressate - secondo cui l'autonomia dei sistemi di intelligenza artificiale renderebbe necessaria l'elaborazione di categorie giuridiche nuove, con l'effetto pratico di attenuare la responsabilità di chi quei sistemi progetta e utilizza. La Corte ricorda che la responsabilità è delle persone. L'intelligenza artificiale resta software: complesso quanto si voglia, ma il cui funzionamento è determinato da scelte umane che ne comportano l'assunzione delle conseguenze.

**Il profilo critico: la responsabilità da progettazione**

La decisione, tuttavia, non affronta il nodo centrale. Che ad accedere al sito sia stato l'utente è affermazione formalmente corretta. Ma il modo in cui Comet è progettato e opera è stato deliberato da Perplexity, che ha strutturato l'interazione in modo da rendere possibile - anzi, ordinaria - quella condotta. Il precedente pertinente è A&M Records, Inc. v. Napster, deciso nel 2001 dal medesimo Ninth Circuit: l'assenza di sistemi idonei a verificare il rispetto del diritto d'autore fondò la responsabilità indiretta dello sviluppatore per quanto veniva compiuto attraverso il software. Il principio è quello della responsabilità da progettazione, oggi al centro del contenzioso statunitense contro le piattaforme social - dove si discute non dell'errore, ma della scelta deliberata di architetture destinate a produrre determinati effetti. Va aggiunto un rilievo ulteriore, che la sentenza non tratta. Non esiste un diritto a utilizzare determinate funzionalità su risorse di terzi. Che un operatore renda disponibile un software funzionante in un certo modo non implica che i titolari delle infrastrutture debbano accettare di interagirvi. Amazon era pienamente legittimata a pretendere che l'assistente fosse riconoscibile e, come tale, bloccabile.

## Amazon v. Perplexity

La Corte d'appello federale attribuisce all'utente la responsabilità dell'agente. E lascia aperto il vero problema.

**Il raffronto con l'impostazione europea**

Il modello che si va delineando oltreoceano procede per via giurisprudenziale e distingue due piani: la responsabilità dell'utente per l'uso dello strumento e quella del produttore per le scelte architetturali. L'ordinamento europeo - e segnatamente quello italiano, dopo i decreti attuativi del 5 agosto 2026 - ha percorso la via normativa, con l'art. 15 AI Act sulla robustezza dei sistemi, il nuovo art. 437-bis c.p. sull'omissione delle misure di sicurezza, la presunzione del nesso causale nei giudizi risarcitori. Le due strade convergono su un punto: chi progetta un sistema capace di operare autonomamente risponde delle capacità che gli ha conferito e dei limiti che non ha predisposto. Il diritto europeo lo ha scritto. Le corti americane lo stanno scrivendo. Nessuna delle due impostazioni consente di trasferire la responsabilità sull'algoritmo.

---

Allinea
Avvera Compliance Review
**Settembre 2026**

## Sanctions Avvera

La piattaforma digitale che automatizza la verifica di clienti e fornitori rispetto alle liste sanzionatorie dell'Unione Europea

L'evoluzione della normativa europea sulle misure restrittive impone alle imprese di rafforzare i propri sistemi di controllo e prevenzione, anche alla luce dell'ampliamento dei rischi rilevanti ai sensi del D.Lgs. 231/2001. Sanctions Avvera è il portale digitale che permette di controllare istantaneamente se una controparte è sottoposta a sanzioni UE. Inserendo il nominativo di un cliente, fornitore o altro soggetto, la piattaforma effettua in tempo reale il confronto con tutte le fonti sanzionatorie disponibili e restituisce un esito chiaro e strutturato, con le informazioni rilevanti sul regime sanzionatorio applicato. Sanctions Avvera aiuta le aziende a prevenire il rischio di rapporti con soggetti sottoposti a misure restrittive UE, rafforzando i presidi di compliance 231/2001. La piattaforma è disponibile in modalità SaaS oppure on-premises per essere integrata nei sistemi aziendali esistenti tramite API. Grazie all'integrazione con il database Sanction Tracker, Sanctions Avvera consente di accedere a informazioni costantemente aggiornate e di ottenere risultati certi e immediati.



Allinea
Avvera Compliance Review
Settembre 2026

# Cyber Resilience Act

## A chi si applica, quali obblighi introduce e quali sono le scadenze

Il Cyber Resilience Act (CRA), Regolamento (UE) 2024/2847, introduce nell'Unione europea un quadro orizzontale di requisiti di cybersecurity per i prodotti con elementi digitali. A differenza di normative come la NIS2, che si concentra principalmente su determinate categorie di soggetti e servizi, il CRA guarda soprattutto al prodotto e alla sua sicurezza lungo il ciclo di vita. Il regolamento è entrato in vigore il 10 dicembre 2024. La maggior parte degli obblighi si applicherà dall'11 dicembre 2027, ma alcune disposizioni sono già operative: in particolare, gli obblighi di reporting dell'art. 14 si applicano dall'11 settembre 2026. Strategia Digitale Europea+1

**A chi si applica il CRA?**
Il punto di partenza è il concetto di **"prodotto con elementi digitali".** Si tratta, in sostanza, di un prodotto hardware o software e delle relative soluzioni di trattamento dati a distanza, compresi componenti hardware o software immessi sul mercato separatamente, quando la finalità prevista o l'uso ragionevolmente prevedibile comprende una connessione, diretta o indiretta, logica o fisica, a un dispositivo o a una rete. Il perimetro è quindi molto ampio e può comprendere, tra gli altri, software, sistemi operativi, applicazioni, dispositivi IoT, router, switch, telecamere, sistemi embedded, componenti hardware e software e prodotti di cybersecurity. Gli obblighi principali gravano sui seguenti soggetti.

*"Il CRA introduce una vera e propria responsabilità di vulnerability handling durante il ciclo di vita del prodotto"*

**Fabbricanti**
È il soggetto centrale del CRA. È considerato fabbricante chi sviluppa o produce un prodotto, oppure ne commissiona lo sviluppo o la produzione, e lo commercializza con il proprio nome o marchio, anche se il prodotto è fornito gratuitamente. EUR-Lex Il fabbricante deve assicurare che il prodotto sia progettato, sviluppato e prodotto nel rispetto dei requisiti essenziali di cybersecurity e deve effettuare una valutazione documentata dei rischi di cybersecurity. Gli obblighi non si esauriscono al momento dell'immissione sul mercato: il CRA introduce infatti una vera e propria responsabilità di **vulnerability handling durante il ciclo di vita del prodotto.**

**Importatori**
L'importatore UE di un prodotto fabbricato da un soggetto extra-UE deve svolgere specifici controlli prima dell'immissione sul mercato, verificando, tra l'altro, la conformity assessment, la documentazione tecnica, la marcatura CE, la dichiarazione UE di conformità e le informazioni per l'utilizzatore. Se viene a conoscenza di una vulnerabilità, deve informare senza indebito ritardo il fabbricante; in presenza di un rischio significativo di cybersecurity sono previsti ulteriori obblighi nei confronti delle autorità di vigilanza.

**Distributori**
Anche i distributori sono soggetti a obblighi di due diligence. Devono, tra l'altro, verificare la presenza della marcatura CE e alcuni elementi relativi agli obblighi del fabbricante e dell'importatore, nonché adottare misure correttive quando emergano problemi di conformità o rischi significativi.

**Soggetti che modificano sostanzialmente un prodotto**
Particolare attenzione deve essere prestata alle modifiche successive alla prima immissione sul mercato. Un soggetto diverso dal fabbricante, importatore o distributore che effettua una **modifica sostanziale** e mette il prodotto a disposizione sul mercato può essere considerato fabbricante ai fini del CRA e assumere gli obblighi degli artt. 13 e 14 per la parte modificata o, in determinate circostanze, per l'intero prodotto.

# Cyber Resilience Act

## A chi si applica, quali obblighi introduce e quali sono le scadenze

**Quali prodotti sono particolarmente interessati?**
Il CRA si applica, in linea di principio, ai prodotti con elementi digitali che rientrano nel suo perimetro generale. Alcune categorie sono tuttavia considerate più rischiose e sono sottoposte a procedure di valutazione della conformità più rigorose.
Tra i **prodotti importanti di Classe** I rientrano, ad esempio, sistemi di gestione dell'identità e degli accessi privilegiati, password manager, software antimalware, VPN, sistemi di network management, SIEM, sistemi PKI, sistemi operativi, router, modem e switch, nonché alcuni prodotti smart home e wearable. La **Classe II** comprende, tra gli altri, hypervisor e container runtime, firewall, sistemi di intrusion detection/prevention e alcuni microprocessori e microcontrollori tamper-resistant. L'Allegato IV individua inoltre alcune categorie di **prodotti critici**, tra cui determinati hardware security devices, smart-meter gateways e smartcard/secure elements.
La classificazione è importante soprattutto perché determina la procedura di **conformity assessment**. Per i prodotti ordinari può essere sufficiente, in determinate condizioni, il controllo interno; per i prodotti importanti di Classe I e soprattutto di Classe II sono previste procedure più rigorose, con coinvolgimento di organismi terzi nei casi previsti dal regolamento.

**I principali obblighi dei fabbricanti**
Il CRA introduce un insieme di obblighi che interessano tanto la fase di progettazione quanto quella successiva all'immissione sul mercato. Tra i principali:

- effettuare e documentare una **cybersecurity risk assessment**;
- progettare e sviluppare il prodotto secondo principi di sicurezza by design e by default;
- identificare e gestire le vulnerabilità;
- predisporre una policy di **coordinated vulnerability disclosure**;
- predisporre un punto di contatto per la segnalazione delle vulnerabilità;
- effettuare test e revisioni periodiche della sicurezza;
- predisporre meccanismi sicuri per la distribuzione degli aggiornamenti;
- fornire tempestivamente gli aggiornamenti di sicurezza;
- predisporre la documentazione tecnica;
- effettuare la procedura di valutazione della conformità applicabile;
- redigere la dichiarazione UE di conformità;
- apporre la marcatura CE quando richiesta;
- fornire agli utenti informazioni e istruzioni per l'uso sicuro del prodotto;
- comunicare chiaramente il periodo di assistenza del prodotto. Strategia Digitale Europea+1.



Particolarmente significativo è il **support period**: il fabbricante deve garantire una gestione efficace delle vulnerabilità per il periodo in cui il prodotto è ragionevolmente atteso in uso. Il periodo deve essere, in linea generale, di almeno cinque anni; se il prodotto è ragionevolmente destinato a essere utilizzato per meno di cinque anni, il periodo può corrispondere alla durata prevista di utilizzo. Gli aggiornamenti di sicurezza devono essere distribuiti senza ritardo e, salvo l'eccezione prevista per determinati prodotti su misura destinati a utenti professionali, gratuitamente. Il CRA richiede inoltre che il fabbricante identifichi e documenti vulnerabilità e componenti, anche attraverso una software bill of materials (SBOM) in formato machine-readable, almeno per le dipendenze di primo livello.

# Cyber Resilience Act

## A chi si applica, quali obblighi introduce e quali sono le scadenze

**Il nuovo obbligo di reporting: già operativo**

L'aspetto più urgente, perché già applicabile, è l'art. 14. Dal **11 settembre 2026**, i fabbricanti devono notificare le:

- **actively exploited vulnerabilities**, ossia vulnerabilità contenute nel prodotto che risultano essere attivamente sfruttate;
- **severe incidents**, cioè incidenti gravi che incidono sulla sicurezza del prodotto.

La notifica deve essere effettuata attraverso la **Single Reporting Platform (SRP)** gestita da ENISA. I termini sono particolarmente stringenti:

- entro 24 ore dalla conoscenza: early warning;
- entro 72 ore: notifica completa;
- per una vulnerabilità attivamente sfruttata, entro 14 giorni dalla disponibilità della misura correttiva: relazione finale;
- per un incidente grave, entro un mese dalla notifica delle 72 ore: relazione finale.

Questo rende opportuno, già oggi, integrare il CRA nei processi di incident response e vulnerability management dell'azienda. Per le microimprese e piccole imprese esiste una specifica deroga alle sanzioni amministrative per il mancato rispetto del termine di 24 ore previsto dall'art. 14, ma l'obbligo di reporting resta.

**E il software open source?**

Il CRA introduce una disciplina particolare per il free and open-source software.
Il software open source non commercializzato non è automaticamente equiparato a un prodotto commerciale. Tuttavia, il regolamento introduce la figura dell'open-source software steward: un soggetto giuridico che fornisce supporto sistematico e continuativo allo sviluppo di determinati prodotti open source destinati ad attività commerciali. Gli steward sono soggetti a obblighi specifici, tra cui una cybersecurity policy e attività di vulnerability handling. Gli obblighi di reporting dell'art. 24(3) si applicheranno dall'11 dicembre 2027.

**SaaS e cloud: attenzione alle semplificazioni**

Non è corretto affermare che "tutto il software" o "tutto il cloud" rientri nel CRA.
Un SaaS puro, in linea generale, non è un prodotto con elementi digitali soggetto al CRA. Tuttavia, una soluzione di trattamento dati a distanza può rientrare nel regolamento quando il software è sviluppato dal fabbricante o sotto la sua responsabilità e la sua assenza impedirebbe al prodotto di svolgere una delle proprie funzioni.
Un esempio è una smart home device la cui funzionalità dipende da un servizio cloud sviluppato dal relativo fabbricante. Al contrario, i servizi cloud generici non necessari al funzionamento di un prodotto non ricadono, per questo solo fatto, nel CRA.



**Le principali esclusioni**

Il CRA non si applica, tra gli altri, a determinati prodotti già disciplinati da normative UE settoriali, tra cui dispositivi medici e dispositivi medico-diagnostici in vitro, determinati prodotti automotive e prodotti aeronautici certificati secondo il quadro normativo indicato dal regolamento. Sono inoltre previste esclusioni per determinate apparecchiature marittime, pezzi di ricambio identici e prodotti sviluppati o modificati esclusivamente per finalità di sicurezza nazionale o difesa o per trattare informazioni classificate.

# Cyber Resilience Act

## A chi si applica, quali obblighi introduce e quali sono le scadenze

**Le scadenze da ricordare**

| Data | Cosa succede |
|---|---|
| 10 dicembre 2024 | Entrata in vigore del CRA |
| 11 giugno 2026 | Si applicano le disposizioni del Capo IV relative alla notifica degli organismi di valutazione della conformità |
| 11 settembre 2026 | Diventano applicabili gli obblighi di reporting dell'art. 14 |
| 11 dicembre 2027 | Piena applicazione della maggior parte del CRA |
| 11 dicembre 2027 | Si applicano anche gli obblighi di reporting specifici degli open-source software stewards |

Una regola transitoria merita particolare attenzione: i prodotti con elementi digitali immessi sul mercato prima dell'11 dicembre 2027 sono generalmente assoggettati ai requisiti del CRA solo se, a partire da tale data, sono oggetto di una modifica sostanziale. Gli obblighi dell'art. 14, invece, si applicano anche ai prodotti già messi a disposizione sul mercato prima dell'11 dicembre 2027.

**Cosa dovrebbero fare oggi le imprese?**
Per un'impresa che potrebbe rientrare nel CRA, il percorso di compliance dovrebbe partire almeno da questi passaggi:

- **Mappare i prodotti** hardware e software commercializzati nell'UE.
- **Identificare il ruolo** dell'impresa: fabbricante, importatore, distributore o altro soggetto.
- Verificare **scope ed esclusioni.**
- Classificare i prodotti come ordinari, importanti Classe I/II o critici.
- Effettuare una **gap analysis** rispetto all'Allegato I.
- Formalizzare vulnerability management e coordinated vulnerability disclosure.
- Definire il support period e la relativa comunicazione agli utenti.
- Verificare documentazione tecnica, conformity assessment, CE marking e dichiarazione UE di conformità.
- Integrare il CRA nei processi di **incident response**.
- Per i fabbricanti, predisporre immediatamente il processo di reporting tramite la Single Reporting Platform di ENISA.
- Rivedere i contratti con sviluppatori, fornitori e produttori di componenti.
- Coordinare gli obblighi CRA con quelli derivanti da **GDPR, NIS2, DORA e altre normative settoriali applicabili.**



## Cyber Resilience Act

A chi si applica, quali obblighi introduce e quali sono le scadenze

**CRA e GDPR: un'intersezione importante**

Per i professionisti della data protection, il CRA presenta un punto di particolare interesse: molte delle attività richieste dal regolamento possono essere coordinate con processi già esistenti in materia di sicurezza dei dati personali. Cybersecurity risk assessment, vulnerability management, incident response, gestione dei fornitori, security by design e gestione degli aggiornamenti possono infatti interagire con gli obblighi derivanti dal GDPR, pur rimanendo obblighi giuridicamente distinti. Il CRA non è quindi una "nuova versione del GDPR cybersecurity": è un regime autonomo di product cybersecurity, che si aggiunge agli altri framework applicabili all'impresa. Per molte software house, produttori IoT, aziende che sviluppano sistemi embedded e imprese che importano prodotti tecnologici da Paesi extra-UE, il 2026 rappresenta quindi il momento opportuno per avviare lo screening e non il momento per attendere l'11 dicembre 2027.

---

Allinea

Avvera Compliance Review

**Settembre 2026**

# Avvera alla Scuola Nazionale di Educazione Civica di Palazzo Montecitorio

Lucia Ruggero, Avvocato ed esperta del nostro team, ha partecipato all'iniziativa della Fondazione Campus Montecitorio, con un intervento dedicato alle sfide legate all'evoluzione dell'intelligenza artificiale e alle sue implicazioni in termini di sicurezza, responsabilità e controllo umano. Al centro del suo contributo, il concetto di "human security" applicato all'AI e tre aspetti fondamentali per governare sistemi sempre più autonomi: riconoscere tempestivamente eventuali anomalie, definire con chiarezza le responsabilità legate alle loro azioni e garantire trasparenza nella gestione degli incidenti. La partecipazione all'iniziativa ha rappresentato un'importante occasione di confronto sul rapporto tra innovazione tecnologica, responsabilità e tutela delle persone, all'interno di un contesto istituzionale dedicato alla formazione e alla cultura civica.

*"Il CRA è un regime autonomo di product cybersecurity, che si aggiunge agli altri framework applicabili all'impresa"*



Allinea
Avvera Compliance Review
Settembre 2026

# Frodi con voce clonata

## Chi risponde quando è il titolare ad autorizzare

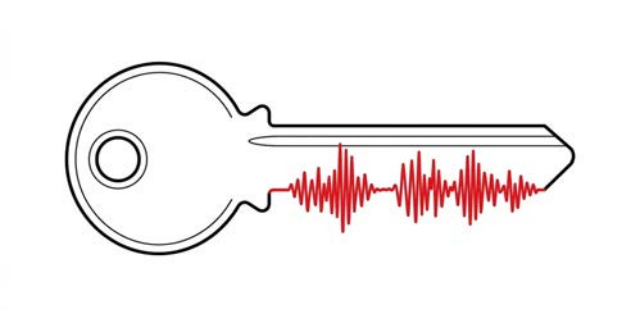
Nel febbraio 2026 dalla tesoreria di Fideuram, istituto bancario del gruppo intesa San Paolo, escono in poche ore circa 95 milioni di euro, diretti soprattutto verso Cina e Hong Kong. L'allora presidente è convinto di eseguire una richiesta urgente dell'amministratore delegato della capogruppo. Oltre 40 milioni vengono bloccati in Cina, 13 sequestrati in Portogallo. Fra i 36 e i 39 non sono stati recuperati. La tecnica usata in questo caso funziona allo stesso modo contro qualunque impresa o privato, e pone la questione più difficile della materia: chi risponde quando è il titolare ad autorizzare?

**La dinamica**

Un messaggio WhatsApp attribuito a un vertice aziendale chiede bonifici urgenti per un'operazione riservata. Segue una telefonata di conferma con la voce, clonata con l'intelligenza artificiale, di un professionista che la vittima conosce. Poi arrivano email con documenti e coordinate. Ogni canale conferma il precedente, e la verifica incrociata è neutralizzata proprio perché il secondo canale è quello chiamato a validare il primo.

**La distinzione decisiva**

Nell'operazione non autorizzata l'utente è ben tutelato. Gli artt. 10 e 11 del D.Lgs. 11/2010 (attuazione della direttiva PSD2) pongono sul prestatore l'onere di provare l'autenticazione. La Cassazione, con la sentenza n. 10638/2016, ha ricondotto il rischio di furto delle credenziali alla responsabilità dell'intermediario, richiamando l'art. 2050 c.c. Nella frode con voce clonata, però, nessuno ruba le credenziali: il titolare le usa di persona. Il consenso c'è, e il rimborso non è automatico.



**Cosa resta al pagatore**

La tutela si sposta sulla diligenza professionale dell'intermediario (art. 1176, co. 2, c.c.), in particolare sul monitoraggio delle anomalie: importo inusuale, beneficiario nuovo, giurisdizione estranea all'operatività del cliente, urgenza sospetta. Dall'altro lato pesa il concorso del pagatore (art. 1227 c.c.), che può ridurre o escludere il risarcimento. Conta anche chi paga. Consumatori e microimprese godono della disciplina piena. Per le altre imprese l'art. 2, co. 4, del D.Lgs. 11/2010 consente di derogarvi per contratto, onere della prova compreso.

**La voce non autentica più**

L'autenticazione forte dell'art. 97 D.Lgs. 11/2010 protegge dall'uso altrui delle credenziali, non dall'inganno del titolare. E il riconoscimento della voce di una persona nota, per decenni una verifica implicita, oggi non vale più nulla. Poiché quella verifica è quasi sempre una prassi interna del cliente, l'impresa che continua ad affidarvisi espone anzitutto sé stessa a una contestazione di colpa organizzativa.

**La verifica del beneficiario**

Dal 9 ottobre 2025 l'art. 5-quater del Reg. (UE) 260/2012 impone alle banche di confrontare IBAN e nome del beneficiario nei bonifici in euro. L'esito non blocca il pagamento, ma pesa. L'avviso ignorato ricade sul pagatore. Se invece la banca non offre la verifica e ciò causa un'esecuzione inesatta, deve rimborsare l'importo. Il servizio non copre però i bonifici extra-UE, come quelli del caso Fideuram, e un truffatore al telefono può convincere la vittima a ignorare l'avviso.

## Frodi con voce clonata

### Chi risponde quando è il titolare ad autorizzare

**I profili penali**

La truffa resta regolamentata dall'art. 640 c.p.. La L. 132/2025 ha però introdotto un'aggravante comune per l'uso di sistemi di AI come mezzo insidioso: l'art. 61 c.p. n. 11-undecies. Inoltre, l'art. 612-quater c.p. punisce chi cagiona un danno ingiusto cedendo o diffondendo voci falsificate con l'AI. La persona clonata può quindi essere persona offesa, purché subisca un danno proprio.

**Contromisure**

La difesa non è percettiva, ma organizzativa. Richiamare il numero ufficiale anziché rispondere al chiamante. Una seconda firma affidata a chi non dipende da chi dispone. Tempi di attesa incomprimibili verso giurisdizioni a rischio. E, a frode avvenuta, richiamo del bonifico e denuncia nelle prime ore.

---

Allinea
Avvera Compliance Review

## Intelligenza artificiale e responsabilità degli enti

### Il D.Lgs. 9 settembre 2026, n. 160 amplia i reati-presupposto della responsabilità ex D.Lgs. 231/2001




È stato pubblicato nella Gazzetta Ufficiale n. 214 del 15 settembre 2026 il D. Lgs. 9 settembre 2026, n. 160 ("Decreto"), recante disposizioni di adeguamento della normativa nazionale al Regolamento (UE) 2024/1689 – AI Act, con particolare riferimento all'utilizzo dei sistemi di intelligenza artificiale nell'ambito delle attività di polizia, nonché ai profili di responsabilità civile e penale connessi al loro utilizzo. Il Decreto è entrato in vigore il 30 settembre 2026. Il provvedimento costituisce attuazione delle deleghe contenute nella Legge 23 settembre 2025, n. 132, con la quale il legislatore italiano aveva già introdotto i principi generali per lo sviluppo e l'utilizzo dei sistemi di intelligenza artificiale e previsto l'adeguamento dell'ordinamento nazionale alla disciplina europea. Particolare rilievo assume, sotto il profilo della responsabilità amministrativa degli enti, l'art. 15 del Decreto, che introduce nel D. Lgs. 231/2001 il nuovo art. 25-vicies – "Reati commessi con l'uso di sistemi di intelligenza artificiale". La disposizione determina l'ingresso nel catalogo dei reati presupposto 231 di due fattispecie penali specificamente connesse all'utilizzo dell'intelligenza artificiale:

**Omessa adozione di Misure di Sicurezza nei Sistemi di Intelligenza Artificiale e alterazione illecita dei Sistemi (art. 437-Bis c.P.)**

Il Decreto introduce nel Codice Penale il nuovo art. 437-bis c.p., volto a presidiare la sicurezza dei sistemi di intelligenza artificiale classificati come ad alto rischio. La disposizione sanziona, in particolare, l'omessa adozione delle misure tecniche di sicurezza previste nelle fasi di progettazione, addestramento, produzione e immissione sul mercato di sistemi di IA ad alto rischio, nonché l'omessa adozione delle necessarie misure di sorveglianza umana, quando da tali omissioni derivi un pericolo per la vita o per l'incolumità pubblica o individuale. Una pena più elevata è prevista quando ne derivi un pericolo per la sicurezza dello Stato. La nuova fattispecie punisce inoltre l'alterazione di sistemi di intelligenza artificiale ad alto rischio quando da tale condotta derivi un analogo pericolo per la vita, l'incolumità o la sicurezza dello Stato. La responsabilità penale può assumere rilievo anche in presenza di colpa gra-

# Intelligenza artificiale e responsabilità degli enti

Il D.Lgs. 9 settembre 2026, n. 160 amplia i reati-presupposto della responsabilità ex D.Lgs. 231/2001

ve con riferimento alle omissioni previste dal primo comma. È inoltre espressamente sanzionato l'utilizzatore professionale di un sistema di IA ad alto rischio che ometta intenzionalmente di adottare le misure di sorveglianza umana, quando ne derivi uno dei pericoli previsti dalla norma. La disposizione assume quindi particolare importanza per le imprese che sviluppano, producono, immettono sul mercato o utilizzano professionalmente sistemi di IA ad alto rischio, rendendo centrali, anche in ottica 231, i presidi relativi alla sicurezza dei sistemi, alla loro supervisione e alla definizione delle responsabilità interne nell'utilizzo degli strumenti di intelligenza artificiale.

**Illecita diffusione di contenuti generati o alterati con sistemi di Intelligenza Artificiale (Art. 612-Quater C.P.)**

Il nuovo art. 25-vicies del D. Lgs. 231/2001 richiama inoltre il delitto di cui all'art. 612-quater c.p., già introdotto dalla Legge n. 132/2025 e ora inserito tra i reati dai quali può derivare la responsabilità amministrativa dell'ente. La fattispecie sanziona chiunque cagioni un danno ingiusto a una persona, cedendo, pubblicando o altrimenti diffondendo, senza il consenso dell'interessato, immagini, video o voci falsificati o alterati mediante sistemi di intelligenza artificiale e idonei a indurre in errore sulla loro autenticità. La pena prevista per la persona fisica è la reclusione da uno a cinque anni. La rilevanza della disposizione in ambito aziendale non riguarda soltanto le attività strettamente tecnologiche. Il rischio può infatti interessare, in funzione delle concrete attività svolte, anche processi quali marketing e comunicazione, produzione di contenuti digitali, social media, utilizzo di immagini o voci di dipendenti, testimonial o terzi e, più in generale, impiego di strumenti di IA generativa nella creazione di contenuti audiovisivi. Particolare attenzione dovrà pertanto essere prestata all'origine dei contenuti utilizzati, all'esistenza delle necessarie autorizzazioni e alla predisposizione di controlli sull'impiego di strumenti in grado di generare o modificare immagini, video e voci.

**Il nuovo regime sanzionatorio per gli enti**

Con l'introduzione dell'art. 25-vicies del D. Lgs. 231/2001, il legislatore ha previsto un regime sanzionatorio particolarmente significativo. Per il reato di cui all'art. 437-bis c.p., relativo all'omessa adozione delle misure di sicurezza e all'alterazione illecita dei sistemi di IA, è prevista a carico dell'ente una sanzione pecuniaria da 600 a 1.000 quote. Per il reato di cui all'art. 612-quater c.p., relativo all'illecita diffusione di contenuti generati o alterati con sistemi di IA, è invece prevista una sanzione pecuniaria da 200 a 700 quote. Per entrambe le fattispecie possono inoltre trovare applicazione le sanzioni interdittive previste dall'art. 9, comma 2, lettere b), c), d) ed e), del D. Lgs. 231/2001, 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.

*"La fattispecie sanziona chiunque cagioni un danno ingiusto a una persona, cedendo, pubblicando diffondendo immagini, video o voci falsificati o alterati mediante sistemi di AI"*

**Implicazioni operative e adempimenti per le società**

L'introduzione dell'art. 25-vicies determina la necessità per le imprese di valutare la propria concreta esposizione ai nuovi rischi 231 connessi all'intelligenza artificiale, tenendo conto sia dei sistemi sviluppati o commercializzati sia degli strumenti di IA utilizzati all'interno dell'organizzazione. Le società interessate dovranno pertanto valutare l'aggiornamento del proprio Modello di Organizzazione, Gestione e Controllo ex D. Lgs. 231/2001, con particolare riferimento alla mappatura delle attività sensibili nelle quali vengono sviluppati, acquistati, configurati o utilizzati sistemi di intelligenza artificiale. In particolare, potranno assumere rilievo la definizione di regole interne per l'utilizzo degli strumenti di IA, l'individuazione dei soggetti autorizzati e delle relative responsabilità, la verifica dei sistemi di IA ad alto rischio eventualmente utilizzati dall'organizzazione, l'adozione delle necessarie misure di sicurezza e di human oversight, nonché l'introduzione di controlli sulla generazione e diffusione di contenuti audiovisivi artificiali o manipolati. Dovranno inoltre essere valutati il rafforzamento dei flussi informativi verso l'Organismo di Vigilanza, l'aggiornamento delle procedure aziendali interessate e l'adozione di specifiche iniziative di formazione e sensibilizzazione del personale in merito ai rischi connessi all'utilizzo dell'intelligenza artificiale.

# Allinea

Avvera Compliance Review

Newsletter Informativa
riservata a clienti e partner
di Avvera

**Settembre**

Tutti i diritti riservati
© AVVERA srl S.B.

AVVERA | SB Società Benefit

Largo Umberto Boccioni 1
21040 Origgio VA
T. +39 02 96515401

Altre sedi
Milano - Pesaro - Udine

avvera.it - info@avvera.it

Immagini: © Adobe Stock, © Deposit Photos, © Esalta