

LA RESPONSABILITÀ DELL'IMPRESA NELL'ERA DELL'INTELLIGENZA ARTIFICIALE



Sacchi & Associati®

MONITORAGGIO, DIFETTO ORGANIZZATIVO E GOVERNANCE
ALGORITMICA NEL NUOVO QUADRO NORMATIVO EUROPEO

Quando l'IA causa un danno, chi risponde?

Dal difetto tecnico del prodotto al difetto organizzativo dell'impresa

L'adozione massiva di sistemi di intelligenza artificiale nei processi produttivi, decisionali e organizzativi dell'impresa ha aperto una stagione di profonda trasformazione del diritto della responsabilità civile. Il legislatore europeo ha spostato il baricentro normativo dal prodotto all'operatore, dal codice al controllo, dall'algoritmo alla governance.

Il **mancato monitoraggio** dei sistemi di IA può costituire un **difetto organizzativo** autonomamente rilevante ai fini della responsabilità civile, idoneo a incidere tanto sull'accertamento della colpa quanto sulla ricostruzione del nesso causale.

«Non si tratta più soltanto di verificare se l'algoritmo funziona correttamente, ma di accertare se l'impresa abbia predisposto un sistema permanente di osservazione, registrazione, analisi e correzione.»

I tre quesiti della ricerca

1

Chi debba rispondere

Dei danni causati da sistemi di IA ad elevata autonomia e processi decisionali opachi.

2

Quale rilevanza assuma il monitoraggio

Se l'omessa vigilanza integri un inadempimento organizzativo idoneo a fondare responsabilità risarcitoria.

3

Come incidano logging e documentazione

Sulla prova del difetto e sul nesso causale, alla luce delle presunzioni della Direttiva 2024/2853.

Tre pilastri normativi

Il perimetro europeo e nazionale della governance dell'IA

EU**REG.(UE) 2024/1689****AI Act**

In vigore dal 1° agosto 2024

- Approccio fondato sul rischio
- Sistema di gestione dei rischi (art. 9)
- Registrazione automatica — logging (art. 12)
- Monitoraggio post-market (art. 72)

IT**LEGGE 132/2025****Legge italiana**

In vigore dal 10 ottobre 2025

- Approccio antropocentrico
- Cybersicurezza lungo il ciclo di vita
- Delega per criteri di imputazione (art. 24)
- Riparto dell'onere della prova

PLD**DIR. (UE) 2024/2853****Product Liability**

Da recepire entro il 9 dicembre 2026

- Software e IA come "prodotto"
- Rilevanza del model drift
- Obbligo di divulgazione prove (art. 9)
- Presunzioni a favore dell'attore (art. 10)

Il fenomeno presenta significative analogie con altri settori del diritto contemporaneo: nella protezione dei dati personali, il principio di **accountability** ha imposto al titolare l'onere di dimostrare la conformità organizzativa delle proprie attività. Analogamente, nel D.Lgs. 231/2001, il corretto assetto organizzativo è elemento essenziale per la valutazione della colpa d'impresa.

Art. 9

GESTIONE DEI RISCHI

Art. 12

LOGGING

Art. 72

POST-MARKET

6 mesi

CONSERVAZIONE LOG
MINIMA

Il ciclo di vita del controllo

Dagli obblighi digestione del rischio al monitoraggio successivo all'immissione sul mercato

ART. 9 AI ACT

Sistema di gestione dei rischi

Processo iterativo continuo lungo l'intero ciclo di vita del sistema ad alto rischio: identificazione, stima e valutazione dei rischi, adozione di misure opportune affinché il rischio residuo sia considerato accettabile.

ART. 12 AI ACT

Registrazione automatica degli eventi (logging)

I sistemi ad alto rischio devono consentire la registrazione automatica degli eventi per l'intera durata del ciclo di vita, a supporto dell'individuazione dei rischi e del monitoraggio post-market.

ART. 72 AI ACT — IN VIGORE DAL 27.07.2026

Monitoraggio post-market

Il fornitore istituisce un sistema che raccoglie, documenta e analizza attivamente e sistematicamente i dati sulle prestazioni del sistema per tutta la durata del suo ciclo di vita.

ART. 26 AI ACT

Obblighi del deployer

Il deployer conserva i log generati automaticamente, nella misura in cui sono sotto il proprio controllo, per un periodo adeguato — almeno sei mesi.

Due soggetti, un solo rischio

La distinzione provider/deployer è cruciale per l'allocazione della responsabilità

Il Provider

Fornitore / sviluppatore del sistema

- Istituisce il sistema di monitoraggio post-market
- Raccoglie e analizza le segnalazioni dei deployer
- Documenta anomalie e incidenti
- Aggiorna il sistema in base ai dati raccolti
- Mantiene la documentazione tecnica (all. IV)

Il Deployer

Utilizzatore nell'ambito della propria organizzazione

- Conserva i log per almeno sei mesi
- Verifica il corretto funzionamento degli output
- Intercetta tempestivamente situazioni di rischio
- Informa il fornitore su eventuali criticità
- Seleziona e forma personale preparato

L'omessa raccolta delle segnalazioni, la mancata analisi degli incidenti o l'assenza di procedure di aggiornamento correttivo possono rappresentare indicatori di una **gestione negligente del rischio**. L'inerzia organizzativa del deployer, in particolare, può determinare un aggravamento del rischio e concorrere causalmente alla produzione del danno.

Dal difetto **tecnico** al difetto **organizzativo**

Il baricentro della responsabilità si sposta dal prodotto alla governance



In questa prospettiva il danno non deriva necessariamente da un errore intrinseco dell'algoritmo, ma dall'assenza di adeguati meccanismi di controllo capaci di individuare e correggere tempestivamente le anomalie. L'impresa che adotta sistemi di IA senza predisporre procedure di audit, supervisione, logging e gestione degli incidenti crea una situazione di rischio causalmente rilevante.

Il difetto organizzativo potrebbe assurgere a **criterio autonomo di imputazione della responsabilità**, analogamente a quanto già avviene nei settori della sicurezza sul lavoro, della protezione dei dati personali e della responsabilità degli enti ex D.Lgs. 231/2001.

«L'impresa che non conserva i log rischia di non poter divulgare le prove richieste, attivando così la presunzione di difetto prevista dall'art. 10 PLD.»

Assetti organizzativi adeguati

Governance dell'IA come parte integrante del dovere di corretta amministrazione

§

Art. 2086, secondo comma, c.c.

Impone all'imprenditore in forma societaria o collettiva il dovere di istituire un assetto organizzativo, amministrativo e contabile adeguato alla natura e alle dimensioni dell'impresa — esteso oggi al governo del rischio algoritmico.

§

D.Lgs. 231/2001

Il Modello di Organizzazione, Gestione e Controllo non è idoneo se non è comunicato, compreso e integrato nei processi organizzativi e nella quotidiana operatività dell'ente — principio esteso alla compliance tecnologica.

§

D.Lgs. 47/2026 (riforma T.U.F.)

Fa esplicito riferimento all'inserimento dell'IA negli assetti organizzativi, amministrativi e contabili delle società quotate.

Le quattro leve della compliance tecnologica

A**Audit & controlli**

Verifiche periodiche documentate sugli output e sulle anomalie del sistema.

L**Log & evidenze**

Conservazione delle registrazioni quale "memoria storica" del sistema di IA.

F**Formazione**

Personale formato a comprendere limiti e criticità degli strumenti utilizzati.

Il peso dei **log** in giudizio

Il regime probatorio della nuova Product Liability Directive (artt. 9-10 PLD)

PASSO 1 – ART. 9 PLD

Obbligo di divulgazione

Su richiesta dell'attore che presenti fatti e prove sufficienti a sostenere la plausibilità della domanda, il convenuto è obbligato a divulgare i pertinenti elementi di prova a sua disposizione — inclusi dati di funzionamento e log.

PASSO 2 – ART. 10, PAR. 2, LETT. A, PLD

Presunzione di difettosità

Se il convenuto omette di divulgare le prove richieste, si presume automaticamente il carattere difettoso del prodotto.

PASSO 3 – ART. 10 PLD

Presunzione del nesso causale

Il nesso causale tra difetto e danno si presume quando sia dimostrata la compatibilità tra la natura del danno e il difetto in questione; in caso di eccessiva complessità tecnica, il giudice può presumere entrambi.

Ne consegue che l'assenza di adeguati sistemi di registrazione e conservazione delle evidenze può assumere un **peso determinante** nell'accertamento giudiziale della responsabilità. La carenza documentale viene progressivamente assimilata a una carenza organizzativa.

Dalla tecnologia all'organizzazione

Dall'algoritmo alla governance: la nuova frontiera della responsabilità civile

Il nuovo quadro normativo europeo si orienta verso una diversa concezione della responsabilità, fondata non soltanto sulla qualità tecnologica del sistema, ma soprattutto sulla **capacità degli operatori economici di governarne i rischi** attraverso adeguati assetti organizzativi. AI Act, PLD e Legge 132/2025 convergono nel valorizzare obblighi di monitoraggio, supervisione umana, logging, documentazione e conservazione delle evidenze.

La responsabilità dell'impresa tende così a spostarsi da una logica esclusivamente reattiva, centrata sul danno già verificatosi, a una **logica preventiva**, fondata sulla capacità di dimostrare di aver esercitato un controllo continuo ed effettivo sui sistemi impiegati.

«L'impresa del futuro non sarà chiamata soltanto a utilizzare sistemi di intelligenza artificiale affidabili, ma soprattutto a dimostrare di aver saputo governare in modo diligente, trasparente e verificabile i rischi generati dalla loro operatività.»

Monitoraggio

ELEMENTO STRUTTURALE DELLA
GOVERNANCE

Accountability

PUNTO D'INCONTRO TECNOLOGIA /
ORGANIZZAZIONE

Prevenzione

NUOVO BARICENTRO DELLA
RESPONSABILITÀ

RIFERIMENTI NORMATIVI

Regolamento (UE) 2024/1689 —AI Act

Parlamento europeo e Consiglio, 13 giugno 2024
· in vigore dal 1°agosto 2024 · artt. 9, 12, 26, 72

Direttiva (UE) 2024/2853 — Product Liability Directive

Parlamento europeo e Consiglio, 23 ottobre 2024
· in vigore dall'8 dicembre 2024 · artt. 7, 9, 10, 11

Legge 23 settembre 2025, n. 132

Disposizioni e deleghe al Governo in materia di intelligenza artificiale
· in vigore dal 10 ottobre 2025 · artt. 3, 24

Art. 2086, secondo comma, c.c.

Come modificato dall'art. 375 D .Lgs. 12 gennaio 2019,n.14
Dovere di assetti organizzativi adeguati

D.Lgs. 8 giugno 2001, n. 231

Disciplina della responsabilità amministrativa degli enti · artt.5,6,7



Sacchi & Associati

Silvano Sacchi & Associati Società tra Avvocati S.r.l.

Via delle Rose, 6 · 24060 Bolgare (BG)

Cod. Fiscale e P.IVA: 04561690167

www.sacchiassociati.it

a cura di Sacchi & Associati — Consulenza AI & Compliance