Norme&TributiPlus

Il Sole 24 ORE

SOCIETÀ ▪ 26 giugno 2026

ISO 42001: lo standard che trasforma la governance dell'intelligenza artificiale in responsabilità misurabile

Lo standard come presidio di accountability: la logica Plan-Do-Check-Act applicata all'AI

di Vincenzo Candido Renna, Laura Spano*

C'è un momento preciso in cui una tecnologia smette di essere un fatto e diventa una questione di diritto. Per l'intelligenza artificiale, quel momento è già qui. Non è un'attesa: è una condizione presente che interpella imprese, professionisti e organi di controllo con un'urgenza che nessuna lista d'attesa normativa può più differire. La domanda non è se **governare i sistemi di AI**, ma con quali strumenti farlo in modo **credibile, documentabile** e – quando necessario – difendibile **davanti a un giudice o a un'autorità di vigilanza**.

È in questo spazio che **ISO/IEC 42001:2023** – *il primo standard internazionale certificabile dedicato ai sistemi di gestione dell'intelligenza artificiale* – acquista un valore che va ben oltre il perimetro tecnico in cui spesso viene confinato. Non si tratta di un protocollo informatico, né di un manuale d'uso per data scientist. È, nella sua **architettura profonda**, uno strumento di governo organizzativo: un *framework* che impone all'ente che lo adotta di definire **politiche, responsabilità, processi di valutazione del rischio** e meccanismi di **miglioramento continuo** con riguardo a qualsiasi sistema AI di cui si avvalga – sia come sviluppatore, sia come utilizzatore.

Il quadro regolatorio: una stratificazione che richiede sintesi

Il professionista legale o economico-finanziario che si affaccia oggi al tema dell'**AI governance** si trova di fronte a una stratificazione normativa di inedita complessità. Al livello europeo, il *Regolamento (UE) 2024/1689 – l'AI Act* – ha introdotto **un sistema di obblighi proporzionato al rischio**: dai divieti assoluti per le applicazioni incompatibili con i diritti fondamentali, fino ai requisiti stringenti di documentazione tecnica, sorveglianza umana e gestione del rischio per i sistemi classificati ad **alto rischio** nei settori **giustizia, finanza, sanità, infrastrutture critiche**. **La piena applicabilità per questi ultimi è fissata all'agosto 2026.**

L'Italia, con la **Legge 23 settembre 2025, n. 132**, si è dotata della prima legge organica nazionale in materia, attuando l'AI Act e individuando le autorità nazionali di vigilanza. **Bankitalia, CONSOB e IVASS** – *come precisato nel recente pacchetto attuativo approvato dal Consiglio dei Ministri* – eserciteranno **funzioni di vigilanza sui sistemi AI ad alto rischio** impiegati dagli **intermediari finanziari**. La legge afferma con chiarezza che l'Italia intende governare l'AI e non subirla; il banco di prova sarà ora la **qualità dei decreti delegati** e l'assetto effettivo della governance nazionale.

A questo si aggiunge il perimetro già consolidato del **D.Lgs. 231/2001**: **l'aggiornamento** del Modello 231 deve intervenire sia sulla **Parte Generale**, integrando i principi di AI governance, sia sulla **Parte Speciale**, introducendo protocolli specifici per le **aree a rischio identificate**, con un ***approval workflow*** che specifichi quali valutazioni siano necessarie prima dell'adozione di nuovi sistemi AI e quali soglie richiedano escalation verso livelli decisionali superiori. **Il GDPR e ISO 27001** completano l'equazione, **vincolando la dimensione dei dati e della sicurezza** delle informazioni che ogni sistema AI inevitabilmente processa.

Sono, questi, sistemi normativi che parlano linguaggi diversi, aggregano obblighi eterogenei e gravano su soggetti che spesso **non dispongono di una bussola tecnico-giuridica unitaria**. È esattamente qui che

***ISO 42001* svolge una funzione sistematica.**

Lo standard come presidio di accountability: la logica Plan-Do-Check-Act applicata all'AI

ISO/IEC 42001 offre una struttura **PLAN-DO-CHECK-ACT** che può rendere **operativi i requisiti legali in modo ripetibile e verificabile**: l'AI Act definisce cosa deve essere raggiunto, mentre ISO 42001 descrive come gestire, documentare e migliorare in modo continuativo un programma di AI governance.

Lo standard impone all'organizzazione di **definire il contesto** in cui opera (*clausola 4*), di stabilire una **politica AI** che sia **coerente con gli obiettivi strategici** (*clausola 5.2*), di condurre una **valutazione del rischio AI** che analizzi non solo i rischi per l'ente ma anche le conseguenze per individui, gruppi e società (*clausola 6.1.2 e 6.1.4*).

Quest'ultimo aspetto – ***l'AI system impact assessment*** – è di rilievo diretto per i professionisti legali: si tratta, nella sostanza, di una procedura documentata di **valutazione dell'impatto dei sistemi AI sui soggetti terzi**, che richiama tanto il registro dei trattamenti del **GDPR** quanto la valutazione d'impatto rilevante per i **sistemi ad alto rischio** ai sensi dell'**AI Act.**

Il punto è cruciale per il tema degli **adeguati assetti** organizzativi, amministrativi e contabili richiesti dal **riformato art. 2086 c.c.**: un'impresa che impieghi sistemi AI rilevanti nei propri processi decisionali, produttivi o finanziari – **senza** aver strutturato un **presidio documentato di governance e controllo** – espone il proprio organo di amministrazione a un **profilo di responsabilità difficilmente sostenibile**. La carenza di un **framework AI** strutturato può oggi configurarsi come **inadeguatezza degli assetti**, con le conseguenti implicazioni in tema di **responsabilità** degli amministratori, del collegio sindacale e degli organismi di vigilanza *ex D.Lgs. 231/2001.*

Perché lo standard volontario diventa una necessità professionale

ISO 42001 e l'AI Act sono **framework complementari, non concorrenti**: la certificazione ISO 42001 fornisce la spina dorsale del sistema di gestione AI, mentre i requisiti dell'AI Act si stratificano sopra, consentendo alle organizzazioni di progettare un unico sistema di governance e riutilizzare controlli ed evidenze tanto per la certificazione quanto per la conformità regolamentare.

La distinzione chiave resta che **l'AI Act** è un **obbligo legale**, mentre **ISO 42001** è uno **standard volontario**; ma lo standard volontario è la grande fondazione che consente di impostare processi identificativi dei framework cogenti applicabili. Chi adotta oggi ISO 42001 non compie un atto di compliance anticipata: compie un **atto di intelligenza strategica**, costruendo un'architettura di accountability che sarà misurabile, auditabile e – se necessario – esibibile in sede di verifica da parte delle autorità di settore.

La *legge 132/2025* rafforza esplicitamente il **principio antropocentrico** come criterio operativo che incide direttamente su **responsabilità, progettazione dei sistemi e modalità di utilizzo**, escludendo che l'AI possa **sostituire l'autonomia decisionale dell'uomo**. *ISO 42001* traduce questo principio in **requisiti concreti**: supervisione umana documentata, valutazione delle conseguenze sui soggetti coinvolti, controllo del ciclo di vita del sistema AI.

Per *l'avvocato d'impresa, per il CFO, per il revisore legale, per il componente dell'OdV 231*, ignorare questa architettura non è più una scelta neutrale. È un **rischio** – *legale, reputazionale, professionale* – che si materializza nella stessa misura in cui i sistemi AI diventano componenti strutturali dei processi aziendali. E quella misura, oggi, è già considerevole.

L'AI governance non è un problema tecnico riservato agli ingegneri del software. È una **questione di responsabilità** – *individuale, organizzativa, istituzionale*.

È la forma contemporanea di quella domanda antichissima che ogni ordinamento giuridico ha sempre dovuto affrontare: *chi risponde, e di che cosa?* ISO 42001 non risolve questa domanda. Ma offre, a chi ha il compito di rispondervi, uno strumento per farlo con **metodo, rigore e tracciabilità**. In un'epoca in cui le

macchine partecipano alle decisioni, costruire sistemi di responsabilità non è un lusso: è il **presupposto della civiltà giuridica.**

**Avv. Vincenzo Candido Renna, Partner 24 ORE e Avv. Laura Spano, Compliance and Sustainability Specialist*

PER SAPERNE DI PIÙ