ANDERSEN

settembre 2026

&Compliance Risk Management

Novità normative e pratiche di governance dei dati e di gestione di rischi d'impresa

Paola Finetto
Partner
paola.finetto@it.andersen.com

Luca Rigotti
Partner
luca.rigotti@it.andersen.com

Hanno collaborato: **Maria Lillà Montagnani**, **Elisa D'Arrigo**, **Nicolò Bottura** e **Giacomo Obetti**

AI Governance

AI Act: le nuove regole di trasparenza per imprese e professionisti

La **trasparenza** costituisce da tempo un presidio essenziale nell'ordinamento europeo, dalla protezione dei dati personali alla tutela dei consumatori. Con l'**AI Act**, tuttavia, assume una funzione specifica: ridurre l'asimmetria informativa creata dall'opacità di molti sistemi di intelligenza artificiale.

Dal 2 agosto 2026 si applicano gli obblighi dell'**art. 50**, sui quali la Commissione europea ha pubblicato specifiche Linee guida.
A differenza degli obblighi previsti per i sistemi ad alto rischio, essi dipendono dalle caratteristiche e dall'uso del sistema.

I **fornitori** di sistemi destinati a interagire direttamente con le persone devono **informarle** che stanno interagendo con un'IA, salvo che ciò sia evidente.
I fornitori di sistemi generativi devono inoltre rendere gli output sintetici rilevabili in formato leggibile dalla macchina.

Specifici doveri ricadono anche sui **deployer**: chi utilizza sistemi di riconoscimento delle emozioni o di categorizzazione biometrica deve informare le persone esposte; chi diffonde deepfake o determinati testi di interesse pubblico generati dall'IA deve dichiararne l'origine artificiale, fatte salve le eccezioni previste.

Non tutti, dunque, sono soggetti agli stessi adempimenti.
Per imprese e professionisti il primo passo è **individuare il proprio ruolo, fornitore o deployer, e mappare sistemi, output e destinatari**.

La trasparenza diventa così un obbligo operativo: sapere chi fa cosa, verso chi e con quali modalità.

D.Lgs. 231/2001

Il Codice Etico: utile strumento anche per disciplinare l'utilizzo dell'IA in azienda

L'intelligenza artificiale sta entrando rapidamente nei processi aziendali, offrendo nuove opportunità di efficienza e innovazione, ma introducendo al contempo rischi inediti: dalla gestione dei dati personali e delle informazioni riservate fino all'utilizzo improprio degli strumenti di IA da parte dei dipendenti.

In questo scenario, il **Codice Etico** può rappresentare uno degli strumenti attraverso cui l'impresa definisce i principi e le regole fondamentali per un utilizzo responsabile dell'intelligenza artificiale.
Non si tratta necessariamente di trasformare il Codice Etico in un documento tecnico.
Al contrario, esso può individuare alcuni **principi generali di condotta**, cui dovranno poi dare concreta attuazione policy, procedure e istruzioni operative.

Tra questi, ad esempio, la trasparenza nell'utilizzo dell'IA, il divieto di inserire informazioni confidenziali in strumenti non autorizzati, la verifica umana degli output e il divieto di utilizzare l'IA per finalità illecite o discriminatorie.

Il Codice Etico può inoltre richiamare espressamente la necessità di utilizzare esclusivamente **strumenti di IA approvati dall'azienda**, nel rispetto dei livelli autorizzativi definiti internamente.
Questa impostazione assume particolare rilevanza anche nell'ambito del **Modello 231**, consentendo di collegare i **principi etici** ai relativi presidi di controllo.
L'uso dell'IA, infatti, può incidere trasversalmente su numerosi processi aziendali e, in determinate circostanze, contribuire alla commissione di reati-presupposto.

Il Codice Etico diventa così non soltanto una dichiarazione di valori, ma una vera **"cornice" di governance dell'IA**, capace di orientare i comportamenti individuali e rafforzare la cultura della compliance, in coordinamento con il sistema di procedure, controlli e responsabilità aziendali.

Privacy | AI | Cyber

Riconoscimento delle emozioni e categorizzazione biometrica: obblighi di informazione

Dal **2 agosto 2026** è applicabile l'**art. 50 dell'AI Act**, che introduce **obblighi di trasparenza** a anche a carico di chi utilizza sistemi di IA nella propria attività professionale sotto la propria autorità (deployer).

Nello specifico, chi impiega sistemi di **riconoscimento delle emozioni** o di **categorizzazione biometrica** deve **informare preventivamente** le persone fisiche esposte del funzionamento del sistema e deve trattare i **dati personali** nel rispetto della normativa in materia di protezione dei dati (GDPR).

In termini operativi, è fondamentale **mappare i sistemi di IA in uso** (ad es. varchi di accesso e controllo presenze, contact center con analisi vocale del tono, retail analytics sui volti dei clienti).
Inoltre, è opportuno verificare se il sistema è soggetto al **divieto** di cui all'art. 5: dal 2 febbraio 2025 sono vietati il riconoscimento delle emozioni sul luogo di lavoro e negli istituti di istruzione (salve le finalità mediche o di sicurezza) e la categorizzazione biometrica diretta a dedurre dati sensibili.

Se i sistemi utilizzati non sono soggetti a divieto, è necessario rendere un'**informativa in modo chiaro**, al più tardi al momento della prima esposizione.
Tale informativa può essere integrata nell'informativa privacy ma non basta una semplice clausola o un richiamo in quanto le due informative devono comunque essere autonome e distinguibili.

Sebbene gli obblighi per i sistemi ad alto rischio siano slittati al 2 dicembre 2027 (Digital Omnibus), la violazione degli obblighi di trasparenza espone già a **sanzioni** fino a 15 milioni di euro o al 3% del fatturato mondiale annuo.
Utile quindi verificare le informative adottate e rivedere le clausole contrattuali presenti nei contratti con i fornitori.

Risk Management

Il valore aggiunto del Risk Manager nella governance dell'IA

La **gestione del rischio** entra spesso in azienda quando il danno si è già manifestato o il pericolo è evidente. Con l'**IA**, però, attendere significa arrivare tardi: siamo in una fase esplorativa, nella quale opportunità e conseguenze evolvono insieme.

Il **Risk Manager** assume un ruolo pionieristico: ricercare, comprendere e anticipare, perché a grandi capacità possono corrispondere impatti altrettanto rilevanti.

Il metodo resta quello del **risk assessment**: identificazione, analisi e valutazione dei rischi, cui segue il **risk treatment**.
L'identificazione non può ridursi a un questionario sui dati.

Il Risk Manager deve "scendere in campo" e confrontarsi con marketing, produzione, amministrazione e tutte le funzioni che usano l'IA, ricostruendo casi d'uso e fonti di rischio.

Contenuti discriminatori, output produttivi non verificati o divulgazione di dati riservati sono **rischi** diversi, ma **interconnessi**.

La disponibilità limitata di dati storici rende difficile stimare probabilità e impatto, ma occorre costruire una **mappa dei rischi** e confrontare il rischio residuo con il **risk appetite**.
Un errore non critico può essere tollerabile se meno frequente di quello umano; non lo è un'esposizione a violazioni dei dati o attacchi informatici.
Il **valore aggiunto** del Risk manager emerge nella formulazione di un piano per il trattamento del rischio.

Diviene quindi fondamentale definire **strumenti GenAI autorizzati**, linee guida e **procedure** interne, misure tecniche per garantire la **sicurezza** dei dati, oltre a **formare** il personale in materia di IA e informare il management. Non semplici divieti, ma strumenti concreti che trasformino il rischio in adozione consapevole e l'IA in **valore per l'impresa**.