NORME ISO ED INTELLIGENZA ARTIFICIALE - LA REGOLAMENTAZIONE TECNICA CHE PREVIENE E CONTIENE I RISCHI

Di Giovanna R. Stumpo

Quello dell'Intelligenza Artificiale e' il tema dell'anno. Si stima infatti che nel 2024 -e così per i prossimi 3 anni-, in Italia, 4 aziende su 10 investiranno in intelligenza artificiale (fonte: Forbes 6.12.2023). E mentre si attende la pubblicazione in GURI del Regolamento europeo sull'Intelligenza Artificiale per assicurare che i sistemi IA immessi sul mercato ed utilizzati nell'Unione siano sicuri, rispettosi dei valori e dei diritti fondamentali comunitari, lo scorso 18 dicembre l'ISO ha pubblicato la ISO/IEC 42001 – Information Technology – Artificial Intelligence – Management System. Primo standard tecnico al mondo che, con le sue disposizioni, fornisce le basi per un sistema di gestione in materia di IA (AIMS- *Artificial Intelligence Management System*), garantistico per gli Operatori di prodotti e servizi dotati di IA, a fronte dalle sue peculiari rischiosità.

NORMA ISO/IEC 42001:2023 – in breve

Impostata secondo la HLS, così da facilitare l'integrazione con altri sistemi di gestione già esistenti (in particolare con: ISO/IEC 27001:2022, ISO/IEC 27701:2019, ISO 9001:2015) la ISO/IEC 42001:2023 "*specifica i requisiti e fornisce indicazioni per stabilire, implementare, mantenere e migliorare continuamente un sistema di gestione dell'AI nel contesto di un'Organizzazione che fornisce o utilizza prodotti o servizi che utilizzano sistemi di intelligenza artificiale*".

Obiettivo fondamentale della norma è di "*supportare un'Organizzazione a sviluppare o utilizzare i sistemi di AI in modo responsabile nel perseguire i propri obiettivi e soddisfare i requisiti normativi applicabili, gli obblighi relativi alle Parti interessate e le aspettative da parte loro*".

Le disposizioni dello standard ISO hanno carattere universale nel settore specifico. La ISO/IEC 42001:2023 si applica infatti "*a qualsiasi Organizzazione, indipendentemente dalle dimensioni, dal tipo e dalla natura, che fornisce o utilizza prodotti o servizi che utilizzano sistemi di intelligenza artificiale.*"

Termini e le definizioni della norma, sono quelli espressi dalla ISO/IEC 22989:2022 – *Information Technology – Artificial Intelligence – Artificial Intelligence concepts and terminology.*

Sul piano dei contenuti, lo standard è strettamente allineato ai requisiti normativi previsti dall'*Artificial Intelligence Act* (AI Act) dell'UE, favorendo quindi le Organizzazioni che vogliono conformarsi al quadro normativo cogente, di rilevante applicazione.

A livello progettuale, la norma tecnica richiede che il sistema di gestione di IA sia integrato con i processi dell'Organizzazione e con la struttura manageriale complessiva. Tematiche specifiche collegate all' IA (in particolare: sicurezza, sorveglianza, equità, trasparenza, qualità dei dati, qualità del sistema AI durante tutto il "ciclo di vita") devono essere prese in considerazione nelle fasi di progettazione e sviluppo del sistema e nell'approccio per processi. Di particolare interesse è anche il quadro delle misure di salvaguardia preventiva che lo standard richiede di considerare a fronte di alcune funzionalità IA, che, per sua natura, sono più pericolose di quelle riscontrabili nei tradizionali sistemi IT (i.e. processo decisionale automatico; capacità analitiche avanzate e di machine learning; capacità apprendimento continuo; possibili deficit di trasparenza e di spiegabilità).

La ISO/IEC 42001:2023 si conforma ai requisiti PDCA ed il *risk based thinking approach* su cui poggia il sistema di gestione dell'IA passa per le fasi obbligati di: "AI risk assessment", "AI risk treatment" e "AI system impact assessment".

Una cura particolareggiata deve essere riservata alla parte di sistema dedicata ai controlli (lo standard tecnico ne contempla 39), da impostare su due macro focus:

i) raggiungere gli obiettivi in relazione all'uso dell'AI;

ii) affrontare le minacce individuate nel processo di valutazione del rischio relativo alla progettazione, allo sviluppo ed al funzionamento del sistema di gestione IA.

In sostanza, è tutto il sistema di gestione che - anche con ricorso alle tecniche applicative del "*management by objectives*"- va tenuto sotto controllo. E ciò, a ciclo continuo; sia quanto alle potenziali evoluzioni di contesto in cui opera l'Organizzazione, sia rispetto agli aspetti di dinamismo e di rapido evolversi - di tempo in tempo - dell'IA.

Il sistema dei controlli ricomprende i seguenti punti specifici:

1. Politiche relative all'AI (anche in allineamento alle altre diverse politiche dell'Organizzazione e relative REV.),
2. Organizzazione interna (ad es. quadro dei ruoli e delle responsabilità),
3. Risorse per i sistemi di AI (ad es. dati, strumenti, risorse umane),
4. Analisi dell'impatto dei sistemi di AI (sia su individui, su gruppi e sulla società; e relativa documentazione),
5. Ciclo di vita del sistema AI,
6. Dati per i sistemi di AI (ad es. acquisizione e preparazione dei dati),
7. Informazioni per le Parti interessate ai sistemi di AI (ad es. comunicazione di ev. incidenti),
8. Utilizzo dei sistemi di AI (uso responsabile ed uso previsto),
9. Rapporti con Terze Parti (ad es. fornitori, clienti).

La ISO/IEC 42001:2023 è corredata di 4 Allegati[1], di cui in particolare l'ANNEX C delinea potenziali obiettivi organizzativi, fonti di rischio e descrizioni che possono considerarsi nella gestione dei rischi legati all'uso dell'IA.

[1] Allegati complementari: ANNEX A: contiene i controlli ovvero le misure da porre in atto per mantenere o modificare un rischio (analogamente a quanto prevede il corrispondente Allegato A della ISO/IEC 27001:2022); ANNEX B: riporta le linee guida per l'applicazione dei controlli definiti nell'allegato A (analogamente alla ISO/IEC 27002:2022 per quanto senza la componente degli attributi); ANNEX D: riguarda gli ambiti e i settori in cui può essere utilizzato un AIMS.

Il livello di dettaglio delle fasi cruciali di analisi e trattamento dei rischi è tuttavia concepito in modo “flessibile” dalla norma, perché l’analisi e la gestione sarà variabile da situazione a situazione. E ciò in dipendenza di numerosi fattori da considerare nella progettazione e nell’implementazione del sistema di gestione a norma ISO/IEC 42001:2023, tra i quali, a titolo indicativo: complessità dell’ambiente, livello di automazione, componente di machine learning, problemi hardware del sistema, stato del sistema nel corso del suo “ciclo di vita”, livello di maturità della tecnologia impiegata.

PER UN QUADRO COMPLETO (RIF. ALTRI STANDARD ISO IN TEMA IA)

- **ISO/IEC 22989:2022** Information technology –Artificial Intelligence
- **ISO/IEC 23053:2022** Framework for Artificial Intelligence (AI) Systems using Machine Learning (ML)
- **ISO/IEC 23894:2023** Information Technology - Artificial Intelligence Guidance on risk management
- **ISO/IEC 5338:2023** Information Technology – Artificial Intelligence system life cycle processes
- **ISO/IEC 5339:2024** Information Technology - Artificial intelligence - Guidance for AI applications
- **ISO/IEC TR 5469:2024** Artificial intelligence - Functional safety and AI systems

PRINCIPALI VANTAGGI DERIVANTI DALLA DECLINAZIONE APPLICATIVA DELLA ISO/IEC 42001:2023

- **Dotazione di un sistema per gestire rischi e cogliere opportunità**
- **Articolare un sistema atto a comprovare l’uso responsabile dell’IA**
- **Fruibilità di una metodologia che garantisce tracciabilità, trasparenza ed affidabilità**
- **Risparmio in termini di costi, con vantaggi in efficienza**
- **Garanzia di uso etico e responsabile dell’IA**
- **Migliore reputazione, con conseguente miglioramento della fiducia per rapporto ad applicazioni IA**
- **Allineamento al quadro normativo e regolamentare applicabile**
- **Gestione efficace dei rischi peculiari IA**