Economy
MODELLI. OPPORTUNITÀ. SOLUZIONI.

L'AI Act e l'eterna ricerca di nuovi standard

La messa a terra dell'Intelligenza Artificiale passa per il delicato equilibrio tra sicurezza e utilità per gli utenti e garanzia di competitività per le imprese. Che senza un aiuto esterno non possono ancora farcela

di Diana Daneluz

L'Intelligenza Artificiale entra in azienda e nelle organizzazioni, che devono adeguarsi. L'**AI Act**, quadro normativo europeo in vigore dal 2 agosto, introduce vari adempimenti secondo la classe di rischio a cui appartiene il sistema di AI: rischio inaccettabile, ove ricadono i sistemi proibiti; alto rischio, es. dispositivi medici; rischio di trasparenza, es. sistemi di informazione; minimo o nessun rischio. Come primo adempimento, dal 2 febbraio 2025 i sistemi AI definiti "proibiti" dovranno essere spenti.

L'AI Act segue il **New Legislative Framework** estendendo al mondo dell'immateriale le regole già in uso per la sicurezza del prodotto: potranno essere immessi sul mercato solo i sistemi AI conformi ai suoi requisiti essenziali.

Tra 113 articoli, 180 "considerando", 13 allegati dell'AI Act gli articoli sono il riferimento per porre in corrispondenza gli standards esistenti, secondo il loro contenuto e i termini definiti. La gap analysis tra AI Act e standards esistenti agevola da parte della Commissione Europea la richiesta di standards armonizzati condivisi da tutti i Paesi dell'Unione: la legislazione definisce i requisiti che la tecnologia deve soddisfare, le norme armonizzate, sviluppate da Enti di Normazione europei, rendono operativi questi requisiti.

Il ruolo degli standards è cruciale: procedure e specifiche che definiscono criteri uniformi per garantire qualità, sicurezza e compatibilità in diversi settori, qui stabiliscono i parametri per sviluppo, uso e implementazione e monitoraggio dei sistemi di AI assicurando che rispettino principi di etica, sicurezza e trasparenza. Un supporto fondamentale al legislatore per un ecosistema normativo coerente, garante di qualità e affidabilità dei sistemi tradizionali in trasformazione e dei sistemi di AI. Il fine è raggiungere eguali condizioni di competitività soprattutto per le piccole e medie imprese e un alto livello di sicurezza e rispetto dei diritti fondamentali per tutti in Europa.

DAL 2 FEBBRAIO 2025 I SISTEMI AI PROIBITI DALL'AI ACT PER LA LORO RISCHIOSITÀ DOVRANNO ESSERE SPENTI

«Per lo sviluppo di standards tecnici per l'AI» spiega **Domenico Squillace**, Technical Relation Leader di **Ibm Italia** (nonché presidente di **Uninfo** (l'Ente Federato di Uni che ha la delega sulla normazione tecnica dell'It), della commissione Uni/Ct 533 AI e della commissione Uni/Ct 535 Quantum Technologies) «sono operativi due comitati: uno a livello internazionale, l'Iso/Iec Jtc 1 Sc 42, e uno a livello europeo, il Cen/Cenelec Jtc 21. In quest'ultimo si sviluppano le norme armonizzate per rendere operativo l'AI Act. In Italia i comitati sono gestiti da Uni Ente italiano di Normazione, tramite la Commissione Uni/Ct 533 presso Uninfo. Per facilitare l'adozione dell'AI e la gestione dei sistemi di AI in Italia, la commissione Uni/Ct 533 ha adottato lo standard Iso/Iec 42001:2023 come norma italiana, la cui traduzione sarà presto disponibile nel catalogo Uni. Si stanno poi definendo i profili professionali relativi all'AI per piani di formazione verso competenze e skills adeguate».

Un ruolo essenziale è quello della formazione per tutti coloro parte attiva nell'adempimento degli obblighi di legge: fornitori, sviluppatori e deployer sono infatti tenuti a garantire (art. 4 AI Act), che il proprio personale soddisfi i requisiti di alfabetizzazione ed educazione, con riferimento ai sistemi di AI in cui operano. Idem per le aziende che decideranno di implementare un Sistema di Gestione AI, in conformità alla Iso/Iec 42001.

«Un contributo essenziale» sottolinea Squillace «è quello offerto dagli esperti italiani allo sviluppo della standardizzazione – e su tutti gli aspetti al vaglio dei gruppi di lavoro, supervisione generale delle attività, strategia, inclusiveness, conformity assessment e risk managemen, governance, qualità dei dati, dataset, bias, trustworthiness, cybersecurity» con il fine di promuovere un'economia nazionale competitiva e so-

Economy
MODELLI. OPPORTUNITÀ. SOLUZIONI.

stenibile, in piena conformità con i principi legislativi e della responsabilità sociale. «Tra gli altri, **Riccardo Mariani**, per la sua leadership nella definizione delle norme Iso/Iec su functional safety, **Renaud Difrancesco** e **Piercosma Bisconti**, project editor delle norme su risk management e trustworthiness, **Valentina Grazia Sapuppo**, alla guida del team che si occupa della Iso/Iec 42001 sui sistemi di AI e sua traduzione in italiano, **Domenico Natale** ed **Andrea Trenta** per la qualità di applicazioni di lachine Learning, Natale con **Luigi Briguglio** sul tema della governance e qualità dei dati per aver contribuito a farne una report tecnica a livello europeo, la cosiddetta Jtc21, anticipando l'importanza dei dati come petrolio del nuovo millennio e base di riferimento di misurazioni valide anche per l'AI».

Proprio Domenico Natale (esperto di standardizzazione Iso/Iec Jtc1 Sc 7 e SC 42, membro Cen-Cenelec Jtc 21 per l'AI, e presidente della Commissione Uni/Ct 504 Ingegneria del software) spiega come gli standards adottati dalle imprese possano supportare l'AI Act verso un equilibrio tra rischi e vantaggi: «L'AI Act traccia la strada su alcune pietre miliari: una AI affidabile e innovativa centrata sull'uomo, la protezione della salute, della sicurezza, dei diritti fondamentali dell'UE, della democrazia e dello Stato di diritto, dell'ambiente contro gli effetti nocivi dei sistemi di AI. Inoltre, una molteplicità di definizioni impongono un grande sforzo di standardizzazione e l'adozione di presidi differenziati per i diversi settori e contesti di intervento».

Agli esperti il compito di fornire nuovi requisiti armonizzati e di offrire al mercato un quadro interconnesso. Fondamentale l'attività di mapping tra AI Act e Standards, ideata nell'ambito della Commissione Uni Ct 533 per la concreta messa a terra dell'impianto del Regolamento AI Act, implementata con il supporto dell'associazione italiana AI Open Mind attiva nell'hosting e sviluppo del progetto grazie ai contributi di Antonio Cappella, Nicola Fabiano e Alessandro Stazi, e patrocinata da realtà nazionali e internazionali. Presentata da Natale per la prima volta in Europa a giugno 2024 all'Università di Bath (UK), è ora in rete, al centro dell'attenzione a livello internazionale, e punta ad un allineamento dei termini e delle definizioni utilizzate nell'articolato normativo del Regolamento con l'ausilio

STANDARD CHIARI E CONDIVISI RIDUCONO I RISCHI E GARANTISCONO FLUIDITÀ E COMPATIBILITÀ TECNOLOGICA

degli standards, unendo disciplina legale e norme tecniche. Al momento sono forniti oltre 350 termini con più di 80 standards, abbinati agli articoli, ai considerando e agli allegati dell'AI Act.

Un'AI pervasiva in tutti i settori economico-sociali, tra rischi e vantaggi, certo, ma per Natale «la bilancia pende verso i secondi: la velocizzazione di servizi ripetitivi, della elaborazione e rappresentatività dei dati in irrefrenabile aumento, l'ottimizzazione di complessità burocratiche, l'approfondimento di scienze naturali e mediche, il progresso nei trasporti intelligenti. Certo, sempre mettendo al centro la protezione dei diritti fondamentali riconosciuti dalla Carta dei diritti fondamentali della UE e dei suoi valori, garantendo trasparenza e funzionamento degli algoritmi. Una buona riuscita dei sistemi di AI dipenderà non solo dall'uso di tecnologie avanzate, ma anche dall'addestramento delle macchine e dal coinvolgimento riconosciuto degli esperti di dominio in grado di trasferire conoscenze ed esperienze dagli uomini alle macchine».

Non mancano rischi: «nell'era attuale in cui le funzionalità del software possono auto-modificarsi e adattarsi, c'è quello del temuto scarso controllo umano con impatto sulla sicurezza. Altro rischio il riproporsi del digital divide per alcuni strati della popolazione a causa della possibile scarsa trasparenza e comprensibilità dei sistemi. L'eventuale utilizzo di dati senza l'adozione di modelli di qualità di riferimento può portare a informazioni mal trasferite alle macchine intelligenti e indurre a risultati errati. Le conseguenze degli automatismi dell'AI sui posti di lavoro, poi, sono da prevedere in anticipo per ridurre i rischi occupazionali, con studi separati nei vari settori economici. E c'è il tema della sostenibilità dell'energia necessaria all'AI, altro importante campo di intervento da tener presente per la mitigazione di rischi economico-sociali».

È, anche, una questione di fiducia: la necessità di standards è particolarmente evidente nell'AI, dove l'assenza di linee guida universali potrebbe comportare rischi significativi. Standards chiari e condivisi contribuiscono non solo a ridurre i rischi, ma anche a garantire che diverse tecnologie possano interagire tra loro in maniera fluida e compatibile. La standardizzazione, pertanto, non è solo un vincolo, ma strumento per favorire innovazione, fiducia di utenti finali e stakeholder in questa nuova evoluzione della scienza dei computer e adozione globale della tecnologia.