Osservatorio ACCREDIA
1 | 2024

Norme tecniche e valutazione della conformità accreditata per lo sviluppo dei sistemi di Intelligenza Artificiale

Executive Summary

In collaborazione con:
cini consorzio interuniversitario nazionale per l'informatica

ACCREDIA
L'ENTE ITALIANO DI ACCREDITAMENTO

Osservatorio Accredia

Direttore editoriale
Gianluca Di Giulio

Coordinamento editoriale
Alessandro Nisi
Francesca Nizzero

Realizzazione grafica
ZERO ONE

Il presente documento è l'Executive Summary dello studio "Norme tecniche e valutazione della conformità accreditata per lo sviluppo dei sistemi di Intelligenza Artificiale" realizzato dall'Osservatorio congiunto "Cybersecurity e Certificazione" costituito da Accredia e dal Laboratorio Nazionale di Artificial Intelligence and Intelligent Systems (AIIS) del Consorzio Interuniversitario Nazionale per l'Informatica (CINI).

Per Accredia: gruppo di lavoro coordinato dall'area Relazioni Istituzionali ed Esterne - Studi e Statistiche e composto da Riccardo Bianconi, Cettina Garufi, Lorenza Guglielmi, Sergio Guzzi, Rosalba Mugno, Alessandro Nisi, Maria Teresa Ruffo, Guglielmo Tozzi.

Per CINI: gruppo di lavoro diretto da Daniele Nardi e composto da Piercosma Bisconti, Stefano Marrone, Lidia Marrassi, Carlo Sansone, Domenico Bloisi.

ACCREDIA
L'Ente Italiano di Accreditamento

Via Guglielmo Saliceto, 7/9
00161 Roma

Tel. +39 06 844099.1
Fax. +39 06 8841199

info@accredia.it
www.accredia.it

Norme tecniche e valutazione della conformità accreditata per lo sviluppo dei sistemi di Intelligenza Artificiale

Introduzione

L'era digitale ha portato con sé numerosi progressi tecnologici, tra cui l'Intelligenza Artificiale (IA), che sta trasformando radicalmente il tessuto della società. Mentre offre possibilità senza precedenti per l'innovazione e il miglioramento della qualità della vita, l'IA solleva anche questioni significative relative alla sicurezza, alla privacy, all'equità e all'etica. Di conseguenza, la regolazione dell'IA è emersa come un campo di interesse accademico, politico e sociale. L'Osservatorio Accredia "Norme tecniche e valutazione della conformità accreditata per lo sviluppo dei sistemi di Intelligenza Artificiale" esplora l'evoluzione della regolazione sull'IA, concentrandosi sul Regolamento UE 2024/1689 (di seguito, anche "Regolamento" o "AI Act") e sviluppa – considerando implicazioni diverse in base agli ambiti di utilizzo dei sistemi di IA – tre Proof of Concept (PoC): due nel contesto biomedicale e uno simulando l'applicazione di una norma tecnica sul Quality Management a una Pubblica Amministrazione. L'analisi identifica un ruolo per l'accreditamento, ruolo che diverrà centrale in tutti quei sistemi di IA per i quali il Regolamento prevede il coinvolgimento di un organismo notificato prima dell'immissione in commercio o della messa in servizio.
Tuttavia, senza un'adeguata competenza tecnico-scientifica, i processi di verifica della conformità non sarebbero attuabili. Questa competenza è essenziale per valutare in modo rigoroso la conformità dei sistemi di IA alle normative, garantendo la sicurezza, l'affidabilità e l'aderenza alle norme tecniche armonizzate che saranno sviluppate dagli Enti di normazione europei (CEN, CENELEC, ETSI).
La conformità al Regolamento richiede, dunque, un elevato grado di conoscenza scientifica e il supporto di soggetti come il Consorzio Interuniversitario Nazionale per l'Informatica (CINI), con il suo Laboratorio Artificial intelligence and Intelligent Systems – con il quale Accredia ha realizzato l'Osservatorio – sarà centrale per garantire sistemi di IA rispondenti ai più elevati standard etici e tecnici.

La definizione di sistema di Intelligenza Artificiale

I sistemi di IA sono l'oggetto di sforzi normativi, sia in Europa sia a livello internazionale, e la loro definizione risulta un compito complesso. La difficoltà nasce dall'intersezione di vari campi disciplinari, dall'evoluzione continua delle tecnologie e dalle differenti applicazioni che abbracciano settori disparati.

La vasta gamma di tecniche e approcci utilizzati nell'IA aggiunge un ulteriore livello di complessità. Il *machine learning*, una delle tecniche più diffuse, si basa sull'analisi di grandi quantità di dati per identificare pattern e fare previsioni. Al suo interno, troviamo sotto-discipline come l'*apprendimento supervisionato, non supervisionato* e *per rinforzo*, ciascuna con i propri metodi e applicazioni. Il *deep learning*, un sottoinsieme del *machine learning*, utilizza reti neurali profonde per elaborare dati complessi come immagini e audio, ma richiede grandi risorse computazionali. La *logica fuzzy*, che permette valori intermedi tra vero e falso, è utile in contesti di incertezza, ma può essere meno precisa rispetto alla logica tradizionale. Gli *algoritmi genetici*, ispirati alla selezione naturale, cercano soluzioni ottimali attraverso processi iterativi, ma possono essere computazionalmente intensivi e non sempre garantiscono la soluzione migliore.
Ogni tecnica ha i suoi punti di forza e debolezza, adattandosi meglio a specifici problemi e applicazioni. Questa diversità tecnologica rende difficile fornire una definizione onnicomprensiva che catturi tutte le sfumature dell'IA.
Proprio per questo, all'interno del Regolamento la definizione di sistema di IA è cambiata numerose volte, passando dalla definizione nella prima versione della bozza di Regolamento – che elencava specifiche tecnologie rientranti nel perimetro di definizione dei sistemi di IA – a una definizione di più alto livello.
Per il Regolamento europeo (art. 3) un sistema di IA è "un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali". Ai fini della ricerca, utilizzeremo pertanto la definizione di sistemi di IA elaborata nell'ambito dell'AI Act.

L'etica dell'Intelligenza Artificiale e l'evoluzione delle metodologie di assessment

La discussione sull'etica dell'IA non è nuova, ma la sua urgenza e complessità sono cresciute in maniera esponenziale con l'avanzare delle tecnologie. Inizialmente, le preoccupazioni etiche erano focalizzate su questioni di bias e discriminazione, ad esempio nel riconoscimento facciale o nei sistemi di decisione algoritmica. Tuttavia, l'attenzione si è ampliata per includere l'impatto più ampio dell'IA sull'autonomia umana, sulla sorveglianza, sul diritto al lavoro e sulla privacy.
Le metodologie di assessment etico sono diventate sempre più sofisticate. Originariamente basate su audit interni e checklist di conformità, queste metodologie si sono evolute verso modelli più integrati e olistici. Gli approcci moderni, come l'ethics-by-design, cercano di anticipare e mitigare i rischi etici prima che i prodotti di IA raggiungano il mercato. Questi strumenti sono vitali per instaurare fiducia tra gli utenti e per garantire che le innovazioni in IA siano responsabili e trasparenti.
La necessità di un quadro normativo ha condotto all'elaborazione di varie iniziative sia a livello nazionale sia internazionale. Uno dei primi tentativi significativi di regolamentare l'IA a livello globale è stato il GDPR (General Data Protection Regulation - Regolamento UE 2016/679) che, sebbene non specificamente focalizzato sull'IA, ha stabilito importanti precedenti in termini di protezione dei dati e accountability algoritmica.

Negli ultimi anni, sono nati specifici framework internazionali destinati a governare l'uso dell'IA. Organizzazioni come l'OCSE e l'UNESCO hanno elaborato linee guida che enfatizzano la trasparenza, la giustizia e il rispetto per i diritti umani nell'impiego dell'IA. Queste linee guida servono come riferimento per i Paesi membri e stimolano l'adozione di normative nazionali coerenti con questi standard internazionali.

Perché un Regolamento europeo sull'Intelligenza Artificiale?

Un momento decisivo nella regolamentazione dell'IA è stato l'introduzione dell'AI Act da parte dell'Unione europea. Il Regolamento ha l'obiettivo di stabilire un quadro normativo armonizzato e proporzionato per regolare l'impiego dell'IA all'interno dell'Unione europea. La *ratio* è fondata sull'idea che l'IA debba essere sviluppata e utilizzata in modo sicuro, etico e rispettoso dei diritti fondamentali e dei valori europei. Di conseguenza, l'atto normativo si propone di classificare i sistemi di IA in base al grado di rischio che essi comportano per la sicurezza e i diritti delle persone, oltre a istituire una serie di requisiti e obblighi per i fornitori, i distributori, gli importatori e gli utilizzatori di tali sistemi.
L'AI Act rappresenta un risultato rilevante nell'evoluzione normativa dell'Unione europea, delineando un quadro giuridico volto a bilanciare la protezione dei diritti fondamentali e delle libertà individuali con la promozione dell'innovazione nel settore dell'IA.
Il percorso legislativo inerente all'AI Act è culminato con la pubblicazione nell'OJEU (Official Journal of European Union) il 12 luglio 2024. La tempistica entro cui il Regolamento dispiegherà i suoi effetti è scalata nel tempo con periodi di 6, 12, 24 e 36 mesi. Ciò riflette la complessità e la portata delle norme delineate, consentendo agli attori interessati di adeguarsi gradualmente ai nuovi obblighi e requisiti. Come già avvenuto con il GDPR, anche per l'AI Act si prevede che l'adeguamento preventivo e spontaneo rivestirà un ruolo fondamentale. La necessità di conformarsi alle disposizioni del Regolamento richiederà un attento esame delle politiche e delle pratiche aziendali, nonché un costante monitoraggio delle evoluzioni normative e tecnologiche nel campo dell'IA.
Con la pubblicazione del Regolamento, le Istituzioni europee si sono poste numerosi obiettivi, tra i quali:

- creare un mercato unico per l'IA favorendo la libera circolazione e il riconoscimento dei sistemi di IA che rispettano le norme dell'UE, promuovendo così l'integrazione e la coerenza nel mercato europeo dell'IA;
- aumentare la fiducia nei sistemi di IA, garantendo che i sistemi di IA siano affidabili, trasparenti e sviluppati secondo un principio di responsabilità, rispettando i principi etici e i diritti fondamentali delle persone;
- prevenire e mitigare i rischi rappresentati dall'IA vietando o limitando l'uso di sistemi di IA che rappresentano un rischio inaccettabile per la sicurezza, la salute, la dignità o l'autonomia delle persone. In tal senso, il Regolamento si propone di proteggere gli individui e i valori democratici da possibili minacce derivanti dall'impiego non regolamentato dell'IA.
- sostenere l'innovazione e l'eccellenza nell'IA fornendo incentivi, finanziamenti e linee guida per lo sviluppo e il dispiegamento di sistemi di IA sicuri ed etici. L'obiettivo è promuovere la crescita e l'avanzamento tecnologico nell'ambito dell'IA, favorendo la cooperazione e il coordinamento tra gli Stati membri, le Istituzioni e le parti interessate al fine di massimizzare i benefici dell'IA per l'intera società europea.

L'approccio al rischio del Regolamento sull'Intelligenza Artificiale

Il Regolamento ruota interamente attorno a un approccio *risk based*, prevedendo una classificazione di quei sistemi di IA considerati ad Alto Rischio.
All'art. 3 del Regolamento viene definito rischio: "la combinazione della probabilità del verificarsi di un danno e la gravità del danno stesso".
Nel valutare il rischio, la Commissione europea tiene conto di diversi criteri, tra i quali, ad esempio, la finalità prevista dal sistema di IA, la misura in cui è usato o verrà impiegato, la portata dell'eventuale impatto negativo (danno) e il numero delle persone che potrebbero essere coinvolte, o l'eventuale previsione di legge di contromisure efficaci volte anche a prevenire o ridurre sostanzialmente i rischi. In generale, i sistemi di IA possono essere suddivisi in quattro categorie di rischio.

Rischio Inaccettabile

I sistemi di IA che presentano un rischio Inaccettabile, si caratterizzano per porsi in netto contrasto con quelli che sono i valori e i principi fondamentali dell'UE, come la democrazia delle Istituzioni, il rispetto della dignità umana e dello stato di diritto.
Proprio perché in contrasto con i fondamenti dell'Unione, questa tipologia di sistemi è vietata o soggetta a severe restrizioni, come nel caso della sorveglianza biometrica in tempo reale per motivi di sicurezza.
Tra i sistemi vietati vi sono, ad esempio, i sistemi di IA che manipolano il comportamento umano coartando o influenzando la volontà degli utenti o che consentono lo *scoring sociale* da parte delle Autorità pubbliche[1].

Alto Rischio

I sistemi di IA ad Alto Rischio (capo III del Regolamento) si caratterizzano per poter avere un impatto sistemico, ossia significativo sui diritti fondamentali o sulla sicurezza degli utenti e dell'ambiente circostante. Tali sistemi sono sottoposti a obblighi e requisiti (elencati alla sezione 2 del capo III) prima di poter essere immessi sul mercato o utilizzati. In dettaglio, sono sistemi ad Alto Rischio quelli che rispettano entrambe le seguenti condizioni:

- rientrano tra i sistemi disciplinati dalla normativa di armonizzazione dell'UE a cui fa riferimento l'allegato I;
- sono soggetti a una valutazione di conformità prima della loro immissione sul mercato o della loro messa in servizio, ai sensi della normativa UE.

Inoltre, l'allegato III contiene un elenco di sistemi ad Alto Rischio, suddividendolo in specifici settori di incidenza, quali, a titolo meramente esemplificativo, quello della gestione delle migrazioni e controllo delle frontiere; dell'occupazione, gestione dei lavoratori e accesso al lavoro autonomo; dell'istruzione e formazione professionale; dell'accesso ai servizi pubblici e privati essenziali.
In ragione dell'esponenziale crescita del livello tecnologico, tale elenco è soggetto a continua revisione, al fine di evitare un disallineamento tra la normazione e la realtà tecnologica raggiunta.

---

[1] *Per l'elenco dei sistemi vietati cfr. art. 5 del Regolamento.*

Va poi sottolineato come un sistema di IA di cui all'allegato III non sia da considerarsi ad Alto Rischio se non presenta un rischio significativo di danno per la salute, la sicurezza o i diritti fondamentali delle persone fisiche.

Rischio Limitato

I sistemi di IA che presentano un rischio Limitato, pur avendo la capacità di influenzare i diritti o le volontà degli utenti, lo fanno in misura minore rispetto ai sistemi ad Alto Rischio. Tali sistemi sono sottoposti a requisiti di trasparenza, aventi la funzione di consentire agli utenti di essere consapevoli del fatto che interagiscono con un sistema di IA e di comprenderne le caratteristiche e le limitazioni. Ciò permetterà agli utenti di esercitare il loro diritto di scegliere se affidarsi o meno al sistema e di capire le possibili conseguenze delle loro scelte. Gli sviluppatori e gli utilizzatori di tali sistemi dovranno anche garantire che le informazioni fornite siano chiare, comprensibili e accessibili. A titolo di esempio, rientrano in questa categoria i sistemi di IA utilizzati per generare o manipolare contenuti audiovisivi (come i *deepfake*), o per fornire suggerimenti personalizzati (come le *chatbot*). In sostanza, l'utente ha il diritto di essere cosciente di stare interagendo con un sistema di IA e non con un essere umano o, per tornare all'esempio dei *deepfake*, di essere consapevole che quell'immagine è stata generata o artefatta tramite un sistema di IA.

Rischio Minimo o Nullo

I sistemi di IA che presentano un rischio Minimo o Nullo si caratterizzano, invece, per il fatto di non aver alcun impatto diretto sui diritti fondamentali o sulla sicurezza delle persone, oltre che per offrire ampi margini di scelta e controllo agli utenti. Laddove un sistema di IA venga categorizzato tra quelli rappresentanti un rischio Minimo o Nullo, lo stesso è da considerarsi libero da qualsiasi obbligo normativo specifico, al fine di rafforzare e incoraggiare l'innovazione e la sperimentazione. Ciò non toglie che anche i sistemi che presentano un rischio Minimo o Nullo devono comunque rispettare le Leggi e i Regolamenti generali applicabili all'IA, come quelli relativi alla protezione dei dati personali, alla concorrenza, alla responsabilità civile o ai diritti dei consumatori. Rientrano in questa categoria i sistemi di IA utilizzati per scopi ludici (come i videogame) o per scopi puramente estetici (come i filtri fotografici).

Le Autorità di notifica e gli organismi notificati e le procedure di valutazione della conformità

Come in altri Regolamenti europei, anche l'AI Act richiama il ruolo delle Autorità di notifica e degli organismi notificati nei casi in cui le esigenze di tutela dei cittadini europei richiedano particolare attenzione. La procedura di notifica è enucleata nella sezione IV del capo III del Regolamento. Gli organismi incaricati della valutazione della conformità devono soddisfare requisiti di indipendenza, imparzialità e competenza per poter essere designati come organismi notificati dall'Autorità competente di ciascuno Stato membro.
Successivamente, sarà compito dell'Autorità di notifica comunicare alla Commissione l'elenco degli organismi notificati.

L'accreditamento è il metodo preferito dall'Unione europea per dimostrare il possesso dei suddetti requisiti, pertanto gli organismi sono incoraggiati a presentare una domanda di notifica con un certificato di accreditamento allegato[2]. In mancanza di questo, l'organismo deve fornire documentazione adeguata a dimostrare la conformità alle disposizioni dell'AI Act. Nell'art. 28 del Regolamento è sancito, inoltre, che gli Stati membri possano optare perché la valutazione e il monitoraggio siano condotti da un organismo nazionale di accreditamento in conformità al Regolamento CE 765/2008.
Gli organismi notificati saranno quindi coinvolti, ai sensi dell'art. 43 del Regolamento, nella valutazione della conformità di alcuni sistemi di IA considerati ad Alto Rischio. In particolare, per i sistemi di IA ad Alto Rischio disciplinati dalla normativa di armonizzazione dell'UE elencata nell'allegato I, sezione A, il fornitore è tenuto a seguire la pertinente procedura di valutazione della conformità prevista da tali atti giuridici.
Il ricorso agli organismi notificati, inoltre, è previsto per i sistemi di IA afferenti alla biometria di cui all'allegato III. Nello specifico, il fornitore dovrà applicare la procedura di valutazione della conformità di cui all'allegato VII (che prevede il coinvolgimento di un organismo notificato) nei seguenti casi:

a) non esistono le norme armonizzate e non sono disponibili le specifiche comuni;
b) il fornitore non ha applicato la norma armonizzata o ne ha applicato solo una parte;
c) esistono le specifiche comuni di cui alla lettera ma il fornitore non le ha applicate;
d) una o più norme armonizzate sono state pubblicate con una limitazione e soltanto sulla parte della norma che è oggetto di limitazione.

Nel caso in cui la procedura di valutazione della conformità, sia essa basata sull'allegato VI (Procedura di valutazione della conformità basata sul controllo interno) o VII (Conformità basata su una valutazione del sistema di gestione della qualità e su una valutazione della documentazione tecnica), abbia esito positivo, potrà essere apposta la marcatura CE, che testimonierà il rispetto della normativa di settore e dall'AI Act. La marcatura dovrà essere apposta in maniera visibile, leggibile e indelebile.
Qualora ciò fosse impossibile o difficilmente realizzabile a causa della natura del sistema di IA, il marchio potrà essere posizionato sull'imballaggio o sui documenti di accompagnamento.
La marcatura CE, ove sia previsto il ricorso di un soggetto terzo nell'ambito della procedura di valutazione della conformità, dovrà essere seguita dal numero di identificazione dell'organismo notificato.

---

[2] L'art. 29 del Regolamento dispone che gli organismi di valutazione della conformità sono tenuti a presentare una richiesta di notifica all'Autorità di notifica ex art. 28 dello Stato membro in cui sono stabilite. La richiesta deve:
• includere una descrizione delle attività di valutazione della conformità;
• contenere dei moduli di valutazione della conformità e dei tipi di sistemi di IA per cui l'organismo dichiara di essere competente;
• essere corredata di un certificato di accreditamento, se disponibile, emesso da un organismo nazionale di accreditamento che attesta la conformità dell'organismo ai requisiti dell'art. 31 del Regolamento, nel quale sono stabiliti requisiti relativi agli organismi notificati.
L'Italia, ha soventemente utilizzato tale opzione, delegando ad Accredia - l'Ente Unico nazionale di accreditamento, tramite apposite Convenzioni, il compito di una valutazione preliminare degli organismi di valutazione della conformità operanti nell'ambito del nuovo quadro legislativo e il successivo monitoraggio.

La funzione delle norme tecniche nella regolamentazione UE in relazione al Regolamento sull'Intelligenza Artificiale

Per promuovere l'armonizzazione nel campo dell'IA, rendendola affidabile e uniforme nel territorio dell'UE, è stato ritenuto necessario affiancare agli obblighi regolamentari anche norme tecniche europee, al fine di coprire le principali aree tecniche coinvolte dall'AI Act.
Per definizione, una norma è una specifica tecnica, adottata da un organismo di normazione riconosciuto, non obbligatoria (Regolamento UE 1025/2012). La normazione, in generale, può avere a oggetto specifiche tecniche di prodotto o di servizio, ossia la redazione di documenti che prescrivono requisiti tecnici che un determinato prodotto, processo, servizio o sistema deve soddisfare. Pertanto, le norme europee costituiscono un insieme di specifiche tecniche e/o criteri stabiliti da un organismo di normazione europeo.
In generale, la normazione europea è organizzata da e per gli stakeholder, rappresentati nazionalmente tramite il Comitato Europeo di Normazione (CEN), il Comitato Europeo di Normazione Elettrotecnica (CENELEC), e la partecipazione diretta degli stakeholder attraverso l'Istituto Europeo di Normazione delle Telecomunicazioni (ETSI). L'intero processo di armonizzazione ruota attorno ai principi riconosciuti dall'Organizzazione Mondiale del Commercio (OMC) nel campo della normazione, ovvero coerenza, trasparenza, apertura, consenso, applicazione volontaria, indipendenza da interessi particolari ed efficienza.
L'obiettivo primario della normazione tecnica nel campo dell'IA consiste nella definizione di specifiche tecniche e/o qualitative a cui i prodotti basati sull'IA, già sul mercato o di futura introduzione, i loro processi produttivi o i servizi forniti, possono conformarsi (su base volontaria) con il proposito di garantire, in modo armonizzato, la sicurezza e l'affidabilità dei sistemi d'IA, nonché la compatibilità e l'interoperabilità con altri prodotti o sistemi.
In linea con il Regolamento UE 1025/2012, le norme che verranno sviluppate nel campo dell'IA avranno un ruolo decisivo nel sostenere l'attuazione della nuova normativa di compliance.
Ai fini dell'analisi del ruolo dell'accreditamento in questa materia, è importante considerare con attenzione la definizione di normativa tecnica armonizzata. Ai sensi dell'art. 2, par. 1, lett. c del Regolamento, si intende per *harmonised standard* (norme armonizzate) "una norma tecnica europea, adottata sulla base di una richiesta della Commissione ai fini dell'applicazione della legislazione dell'Unione sull'armonizzazione".

Rapporto tra Standardization Request e AI Act

L'Osservatorio Accredia sviluppa un'analisi della Standardization Request (SR) redatta dalla Commissione europea ai sensi del Regolamento e pubblicata a maggio 2023. Una nuova richiesta di normazione, aggiornata al contenuto finale del testo dell'AI Act, è attesa entro il 2024. Dato questo presupposto, è bene evidenziare come la SR si muova all'interno del panorama normativo ben definito, da individuarsi in particolare nel Regolamento Standard UE 1025/2012, nella Direttiva UE 1535/2015, nel Regolamento CE 765/2008 e nel Regolamento UE 1020/2019.
Tra le categorie di soggetti coinvolti nel processo di normazione vi sono:

- le ESO (Organizzazioni Europee di Normazione), attualmente CEN e CENELEC con un possibile coinvolgimento futuro dell'ETSI;

- gli NSB (Organismi Nazionali di Normazione), responsabili della produzione di normativa tecnica in ciascuno degli Stati membri, identificati in Italia come CEI e UNI;
- le organizzazioni europee degli stakeholder (portatori di interessi);
- i consulenti per le norme armonizzate.

Avvio del processo di normazione

Nella fase di avvio, la Commissione europea, da cui trae origine la richiesta, rilevata l'esigenza di normazione, identifica le aree d'intervento in cui considera necessario operare. Nello specifico, sviluppa una bozza di richiesta di normazione (SR per le ESO) includendo dettagli sul campo di applicazione, i tempi e i requisiti legali che le norme dovrebbero specificare.
Nel caso dell'AI Act, il tipo di specifica atteso dalle norme tecniche riguarda alcuni articoli del Regolamento, generalmente quelli più tecnici (capo 2, sezione III). Ad esempio, l'art. 15 contiene indicazioni generali sulla necessità di garantire la robustezza, accuratezza e cybersicurezza dei sistemi di IA, ma non stabilisce in che modo. Il ruolo delle norme tecniche, in relazione al Regolamento, è quindi specificare gli articoli del Regolamento con procedure tecniche, fornendo dei requisiti "di basso livello", come ad esempio le metriche per misurare l'accuratezza.

Redazione della bozza delle norme

Una volta approvata e ricevuta la SR, i Comitati Europei di Normazione incaricati avviano le procedure per la stesura delle norme. A seguito della consultazione dei portatori di interessi, dell'effettuazione delle ricerche tecniche necessarie, sarà elaborato il "testo regolamentare", al fine di produrre norme conformi alle richieste espresse dalla Commissione.
Le norme europee sviluppate seguiranno procedure trasparenti e partecipative per garantire la rappresentanza degli interessi di tutti gli attori coinvolti. In particolare, gli NSB sono chiamati a fornire un pool di esperti che si confronteranno nell'ambito di un comitato tecnico.
Per quanto attiene alla SR relativa all'AI Act, si tratterà di un comitato tecnico congiunto tra CEN e CENELEC. Il comitato tecnico formerà, poi, un gruppo di lavoro (working group) di esperti costituito dagli NSB e dagli osservatori al fine di redigere una bozza del documento contenente l'architettura delle norme relative all'AI Act.

Adozione della norma

Completato il processo di redazione della bozza, la norma europea proposta viene sottoposta a un voto tra i membri del CEN, CENELEC o ETSI. I consulenti valutano se le norme rispettano i requisiti contenuti nella SR e, pertanto, se sono adatti a essere pubblicati. I consulenti per le norme armonizzate possono essere coinvolti durante tutto il processo, ma le norme devono superare definitivamente il vaglio di conformità al momento della votazione, in quanto, a seguito della consultazione, possono essere effettuate unicamente variazioni minimali. Nello specifico caso dell'AI Act, i consulenti non saranno interpellati, stante alcune dichiarazioni di DGCNECT (Directorate General Communications Networks, Content and Technology) della Commissione europea rilasciate informalmente durante alcuni workshop pubblici. Una volta che il documento sarà approvato dalla maggioranza dei membri, laddove le norme vengano considerate conformi, verranno pubblicate nell'OJEU divenendo norme armonizzate. Per quanto attiene all'armonizzazione delle norme inerenti all'AI Act, gli NSB saranno responsabili dell'adozione delle norme europee a livello nazionale e dovranno, nel caso sia necessario, eliminare ogni norma che risulti in conflitto con le norme europee realizzate sulla base dei principi sanciti all'interno del Regolamento.

In conclusione, per quanto attiene al rapporto tra AI Act e SR, si comprende come il Regolamento fornisca la cornice di riferimento entro la quale le norme tecniche relative a questa "famiglia" di tecnologie dovranno essere sviluppate.

Proof of Concept

Una parte centrale dell'analisi dell'Osservatorio Accredia riguarda i PoC (Proof of Concept). Ponte tra la teoria normativa e la pratica applicativa, i PoC offrono una piattaforma per testare, in ambiente controllato, l'efficacia e la conformità dei sistemi di IA rispetto alle norme tecniche e consentono di evidenziare un ruolo potenziale per l'accreditamento e le relative certificazioni.
I PoC assumono una significativa rilevanza in quanto strumenti essenziali per comprendere i processi di accreditamento, ispezione e certificazione di tali tecnologie. Questi processi sono fondamentali per garantire che i sistemi di IA non solo aderiscano alle norme di qualità e sicurezza stabilite dalle norme tecniche, ma siano anche implementati in modo da rispettare i rigorosi requisiti dell'AI Act europeo.
L'adozione di linee guida e norme tecniche, come la ISO/IEC TR 24027:2021 e la ISO/IEC 42001:2023 nel contesto dei PoC, serve a illustrare concretamente come i sistemi di IA possano essere progettati e valutati per assicurare che i bias siano minimizzati e che la gestione della qualità sia mantenuta a livelli ottimali. I PoC facilitano l'elaborazione di linee guida dettagliate per le ispezioni, essendo questi capaci di identificare specifiche aree di rischio e di efficacia che gli ispettori possono poi monitorare e valutare. Attraverso i PoC, possono essere sviluppate procedure di verifica più mirate ed efficaci, che si traducono in processi di certificazione più affidabili e trasparenti.
Lo studio dell'Osservatorio illustra due PoC nel contesto biomedicale e uno in una Pubblica Amministrazione. Nel primo caso, i PoC sviluppati riguardano un sistema di IA per la detection del melanoma e uno per la stratificazione dei pazienti con sclerosi multipla, mentre, nel caso della Pubblica Amministrazione, viene simulata l'applicazione di una normativa tecnica sul Quality Management. I PoC in ambito biomedicale non solo hanno dimostrato la capacità dell'IA di supportare le decisioni cliniche, ma sono serviti a dimostrare l'importanza di una procedura che comprende la raccolta e preparazione dei dati, lo sviluppo e la valutazione dei modelli, e infine il rilascio del sistema. In particolare, è stata simulata una procedura di valutazione della conformità di un sistema di IA alla ISO/IEC TR 24027:2021.
Viene infatti presentato un modello di valutazione della conformità a questa linea guida dell'ISO da cui discende una checklist operativa volta, da una parte, a guidare l'attività di verifica dell'organismo notificato e, dall'altra, ad aiutare il fabbricante nell'intero processo di revisione e miglioramento del sistema. La linea guida ISO mira a eliminare potenziali pregiudizi nei sistemi di IA, garantendo che le diagnosi e i trattamenti proposti non siano solo accurati, ma anche equi e imparziali. La verifica di conformità secondo la ISO/IEC TR 24027:2021 è un passaggio cruciale, che assicura che i sistemi di IA rispettino i principi di affidabilità, supportando così l'implementazione dell'AI Act.
L'AI Act richiede che i sistemi di IA siano trasparenti, etici, e che operino senza discriminazioni, integrando requisiti normativi stringenti per prevenire i rischi in materia di diritti fondamentali e sicurezza delle persone. I PoC nel settore sanitario rappresentano quindi non solo un esercizio di conformità tecnica, ma anche un allineamento ai valori e alle norme europee sull'uso etico dell'IA.

Parallelamente, nel settore della Pubblica Amministrazione, il caso di studio condotto con l'INAIL (Istituto Nazionale per l'Assicurazione contro gli Infortuni sul Lavoro) evidenzia l'importanza della norma ISO/IEC 42001:2023 sul Quality Management per i sistemi di IA. Questa norma si concentra sull'implementazione di sistemi di gestione della qualità, fondamentali per garantire che le decisioni prese dai sistemi di IA siano consistenti, riproducibili e affidabili. In un ambiente complesso come quello della Pubblica Amministrazione, dove le decisioni possono avere impatti ampi e significativi sulla vita dei cittadini, l'adeguamento a tali norme assicura che ogni processo decisionale automatizzato sia sottoposto a controlli rigorosi prima di essere implementato.
Questo approccio è particolarmente pertinente nell'ottica dell'AI Act, che sottolinea l'importanza di una gestione adeguata del rischio e della qualità nell'IA. La norma ISO/IEC 42001:2023, quindi, non solo risponde a esigenze tecniche, ma si allinea anche agli obiettivi dell'AI Act per promuovere un utilizzo responsabile dell'IA, basato su elevati standard di qualità. La necessità di aderire a norme tecniche rigorose e riconosciute globalmente è un presupposto non solo per la conformità normativa, ma anche per il rafforzamento della posizione competitiva a livello internazionale nel settore dell'IA.

Il ruolo dell'accreditamento

I PoC evidenziano l'importanza della valutazione di conformità accreditata ai requisiti definiti all'interno del ciclo di sviluppo di un modello di IA, segnatamente nell'ambito biomedicale. La valutazione della conformità accreditata per i dispositivi medici e in particolare per quelli contenenti sistemi di IA richiede imparzialità, competenza e coerente funzionamento dell'organizzazione preposta a tale attività. La valutazione della conformità deve essere posizionata strategicamente prima della fase di rilascio o implementazione, per assicurare che il modello sia conforme ai requisiti normativi e alle aspettative di qualità.
Come sottolineato nell'Osservatorio, è bene differenziare tra un prodotto destinato a essere immesso sul mercato e uno di natura più strettamente di ricerca (prodotto scientifico). Mentre per il primo è indispensabile una valutazione che comprenda aspetti come la sicurezza del paziente, la conformità normativa e l'efficacia clinica, per i prodotti scientifici o di ricerca, la valutazione della conformità normativa non è obbligatoria e l'enfasi potrebbe essere maggiormente posta sulla validità metodologica, l'innovazione e la capacità di contribuire alla base di conoscenza medica.
L'importanza di un processo di valutazione della conformità per i sistemi basati su IA nel settore medico si evidenzia considerando le potenziali conseguenze di un rilascio prematuro di tali tecnologie senza un'adeguata valutazione dei rischi. Una volta che un modello è entrato nel mercato o è stato adottato in contesti clinici, intervenire per correggere difetti o rimuovere il sistema può essere estremamente difficile, costoso e dannoso, anche per gli utilizzatori e i pazienti.
Nel caso dei dispositivi medici e medico-diagnostici in vitro, trattandosi di prodotti, già ora, rientranti nella disciplina dei Regolamenti UE 2017/745 e 2017/746, è prevista, prima dell'immissione sul mercato, la valutazione da parte di un organismo notificato, a seconda della classe di rischio del dispositivo medico stesso. In tale contesto è da ribadire come l'accreditamento rappresenti uno strumento importante per garantire la conformità dei sistemi basati sull'IA.
L'accreditamento contribuisce a garantire l'efficienza, la trasparenza e la qualità dei servizi offerti ai cittadini.

Il rispetto dei requisiti definiti è fondamentale per assicurare che i sistemi di IA siano sviluppati e applicati in maniera sicura, etica e responsabile. Allo stesso tempo l'accreditamento, quale attestazione autorevole di conformità alla normativa tecnica rilevante, aiuta le imprese a raggiungere la conformità al Regolamento. Si tratta certamente di un passaggio centrale per la tutela dei cittadini europei rispetto a una tecnologia con profili di rischio potenzialmente lesivi e in continua evoluzione.

Accredia, in qualità di Ente Unico nazionale di accreditamento designato dal Governo in applicazione del Regolamento europeo 765/2008 e vigilato dal Ministero delle Imprese e del Made in Italy, attesta la competenza e l'imparzialità degli organismi di valutazione della conformità, garantendo la correttezza e la conformità dei processi di verifica e certificazione. Per questo, Accredia può contribuire – insieme alle Istituzioni cui sono state attribuite le funzioni di gestione e controllo dell'IA – a garantire che la famiglia di tali tecnologie sia rispondente ai requisiti stabiliti dall'AI Act. Una collaborazione che, come già avviene per altri beni e servizi, alleggerisce il carico amministrativo delle Pubbliche Amministrazioni e, nel caso di specie, potrebbe rendere maggiormente efficienti le attività di accreditamento e monitoraggio delle attività di valutazione della conformità nell'applicazione dei sistemi di IA.

Osservatorio
ACCREDIA

Via Guglielmo Saliceto, 7/9
00161 Roma

Tel. +39 06 844099.1
Fax. +39 06 8841199

info@accredia.it
www.accredia.it

Scopri di più

ACCREDIA
L'ENTE ITALIANO DI ACCREDITAMENTO