

Giornata di formazione Associazione Nazionale Imprese Assicuratrici

“ Ai Governance e AI compliance: quale impatto dell’Artificial Intelligence Act sul settore assicurativo “

Oreste Pollicino, Professore di costituzionale e diritto della regolazione dell’intelligenza artificiale, Università Bocconi e Founder
www.PollicinoAIadvisory.eu

Buon pomeriggio.

AI governance e AI compliance, quale impatto dell’Artificial Intelligence Act sul settore assicurativo? Il tema è assai attuale. Cercherò di essere il più possibile indolore provando a tradurre un linguaggio che spesso è complesso perché noi giuristi tendiamo a complicarci la vita, in una bussola comprensibile per gli addetti ai lavori

La prima sfida . Cercare innanzitutto di dare un contenuto, un significato a parole, concetti, etichette spesso, che in qualche modo rimangono nell’iperuraneo, nell’etereo giuridico dell’AI ACT e che poi però vanno calate all’interno delle singole aziende non soltanto nel comparto assicurativo. Cosa significa per una compagnia assicurativa calare nella propria policy aziendale concetti come Human in the loop, esplicabilità dell’AI, non discriminazione, trasparenza, AI responsabile?

Sicuramente si deve provare a dare un significato attraverso la scrittura. Io ho provato a dare un mio contributo per questo esercizio con Banca Intesa, collaborando ad una struttura solida di un corpus normativa che dia sostanza a questi concetti attraverso linee guida e regole operative per provare a rispondere a queste domande: chi fa cosa in azienda con riferimento ad AI governance? E con quali strumenti?

Vi è però anche un altro tema che va subito affrontato. Dedurre da un ragionamento corretto conseguenze radicali e quindi errate.

Il ragionamento corretto è stato evidenziato anche dal rapporto Draghi e non mi soffermo, cioè l’ipertrofia regolamentare europea che ha chiaramente degli effetti negativi sulla alimentazione dei processi di innovazione in Europa. Non si può certo con questo però resettare il percorso regolatorio che ha portato all’AI Act. Un percorso che è iniziato nel 2021 ed è finito nel 2024.

Perché in qualche modo non si prende in considerazione, e questo è il primo punto, quella discontinuità tecnologica su cui insisto molto io,

dall'automazione all'autonomia. Dall'automazione all'autonomia: la sfida dell'AI Act tra discontinuità tecnologica e dignità della persona

Perché, in qualche modo, non si prende ancora abbastanza sul serio quella discontinuità tecnologica su cui insisto da tempo: lo slittamento dall'automazione all'autonomia. Questo è, a mio avviso, il primo nodo da affrontare. Non è un caso se il Regolamento europeo è stato, a un certo punto, radicalmente riscritto.

Eppure sono passati solo quattro anni dalla proposta della Commissione nel 2021. Cosa è accaduto nel frattempo? L'esplosione dell'intelligenza artificiale generativa e, con essa, l'affermazione del concetto di autonomia.

Questo passaggio ha imposto di ripensare parti consistenti del testo normativo, nella sua versione finale pubblicata lo scorso anno. Perché? Perché è apparso evidente che il modello europeo non poteva rimanere indifferente a questa accelerazione tecnologica, senza tradire la propria stessa architettura di valori: penso, in primis, alla dignità della persona, alla tutela della sfera individuale. Lo spostamento dall'automazione algoritmica — che implica quantità di dati e opacità di calcolo, ma pur sempre con un residuo margine di controllo umano — all'autonomia delle AI ha richiesto, in alcuni casi, una risposta radicalmente nuova.

Il regolamento europeo, da molti criticato per la sua presunta sproporzione, è la manifestazione di questa reazione. Non è mia intenzione soffermarmi qui sul Regolamento in sé, ma piuttosto evidenziare quali sono, a mio avviso, i profili che occorrerà presidiare, guardando al passato ma soprattutto al futuro, per evitare errori di sottovalutazione che rischiano di costare carissimo. Non tanto — o non solo — in termini sanzionatori, ma sul piano reputazionale e del posizionamento competitivo.

Oggi ci troviamo in un limbo normativo, in una fase di transizione. Pochissimi soggetti italiani hanno sinora avviato un lavoro di preparazione “pre-AI Act”. Penso, ad esempio, a Banca Intesa che, in ambito bancario, ha redatto una normativa interna con linee guida e regole operative capaci di rendere intellegibile la governance algoritmica. E credo che questo sia un suggerimento prezioso, mutatis mutandis, per il comparto assicurativo.

Il nodo di fondo, infatti, è la chiarezza dei ruoli. La vera incognita, dal punto di vista della compliance, è sapere chi fa cosa. Chi fa cosa in aziende che, talvolta, sono veri e propri micro-sistemi statuali.

Il primo tassello di questo mosaico è già in vigore dal febbraio 2025 scorso: si tratta dell'obbligo di formazione e di alfabetizzazione tecnologica. Una misura spesso trascurata, eppure cruciale. Esiste qualche isola virtuosa — penso alle relazioni industriali — che ha iniziato a costruire percorsi formativi adeguati. È essenziale che questo diventi una best practice diffusa.

Quando parliamo di modelli ad alto rischio, è bene intendersi: nel settore assicurativo — come in quello creditizio — il rischio è la regola, non l'eccezione. Ed è proprio questo il cuore del problema. Un modello ad alto rischio non è vietato in quanto tale. È consentito, ma in un regime di gestione e di scommessa consapevole sul rischio stesso. Regolare il futuro implica, in fondo, un atto di scommessa.

Vi sono, certo, modelli di AI esplicitamente vietati. Non perché siano tecnicamente irrealizzabili — pensiamo al riconoscimento emotivo nei colloqui di lavoro — ma perché infrangono un limite invalicabile: la dignità umana. Dal febbraio scorso, meccanismi di questo tipo sono interdetti. La risposta europea è stata un “no” secco, netto. Potreste obiettare che nelle vostre imprese non vi è traccia di tali pratiche. Ma l'unico modo per esserne certi è una mappatura completa. È ben diverso avere la percezione di non adottare social scoring o riconoscimento biometrico in tempo reale, e avere prove documentali che lo certifichino. E questo obbligo di mappatura è già pienamente operativo.

Qui non si tratta solo di sanzioni. Mi preoccupa, piuttosto, il rischio di una inconsapevolezza diffusa. Serve un linguaggio comune tra chi sviluppa tecnologia e chi la governa. Troppo spesso, in azienda, l'IT sa di cosa si parla, mentre altre aree restano escluse da questo lessico tecnico. Pensate, per esempio, a uno strumento come Copilot: quante persone sanno se rientra, o no, nel perimetro dell'AI? Non è una domanda banale: l'AI Act si applica solo a tecnologie che rispettino la definizione di intelligenza artificiale. Automazioni di vecchia generazione restano escluse.

Questa domanda — che tecnologia stiamo utilizzando? — non può essere delegata solo al Legal, all'IT o alla Compliance. Occorre una cabina di regia trasversale, capace di rispondere a questa domanda. Anche perché, nella pratica, spesso convivono automazioni tradizionali e nuove forme di autonomia algoritmica.

Il passo successivo è costruire un modello di AI governance. Questo implica due livelli: linee guida chiare e regole operative puntuali. Le linee guida devono definire chi è responsabile di cosa, chi decide cosa si può fare e come. Non basta affidare il tutto a un'unica area aziendale. Serve un tavolo di

coordinamento, perché — lo dico per esperienza — talvolta manca del tutto un linguaggio condiviso. E se le parole mancano, manca anche la strategia.

Quando si trova un lessico comune, allora si può iniziare a dare concretezza ai principi di AI responsabile, human in the loop, esplicabilità, trasparenza, fairness. Concetti che devono essere calati nel vostro contesto operativo: scritti in 20-30 pagine chiare, non in tomi incomprensibili. Accanto alle linee guida, servono regole operative. Cosa significa? Significa stabilire, in modo verificabile, chi fa cosa. Non basta dire di voler garantire l'esplicabilità: occorre misurare, dimostrare, certificare. A chi? Al regolatore europeo — l'AI Office — ma anche a quelli nazionali: AGID per la notifica, ACN per la vigilanza. Come con il GDPR nel 2018, qui la differenza tra responsabilità e accountability è cruciale: non basta fare, bisogna saperlo dimostrare.

Tutto ciò cambia a seconda del ruolo: provider o deployer. Nel 90% dei casi, le compagnie assicurative sono utilizzatrici di AI. Ma non mancano casi in cui diventano provider, sviluppando modelli proprietari di AI generativa. È evidente che obblighi e oneri cambiano di conseguenza.

A questo proposito, c'è un tema delicatissimo: la valutazione di impatto sui diritti fondamentali. L'articolo 27 dell'AI Act individua in prima fila banche e assicurazioni, insieme ad altri soggetti privati che erogano servizi essenziali. Ma essere in "buona compagnia" — trasporti, energia, telecomunicazioni — non solleva dall'obbligo di fare bene.

Perché questo obbligo? Perché quando la Commissione, nel 2021, concentrava l'attenzione sulla product safety, non poteva prevedere l'irruzione dell'AI generativa. Con l'esplosione di questi modelli, si è compreso che la sicurezza del prodotto non bastava più. Occorreva un'iniezione di tutela dei diritti fondamentali. E così, nell'ultima settimana di negoziato, il Parlamento europeo ha inserito questo obbligo di valutazione d'impatto. È una sfida complessa, certo, ma può trasformarsi in una grande occasione di valorizzazione reputazionale, se interpretata in modo costruttivo.

Di quali diritti parliamo? Dal primo al cinquantesimo articolo della Carta dei Diritti Fondamentali dell'Unione Europea: un Bill of Rights che, anche grazie a Stefano Rodotà, è vincolante dal 2009. Il problema non è sapere quali diritti: è tradurre in pratica questa valutazione. Non esiste un calcolo statico: non si può dare un "punteggio" ex ante. Occorre, piuttosto, un bilanciamento concreto e dinamico. Servono misure qualitative e quantitative, un lavoro di squadra tra legali, data analyst e stakeholder, sindacati inclusi. È qui che si fissa una soglia minima di garanzia, anche tramite la contrattazione collettiva.

Ma tutto questo, senza una certificazione, rischia di rimanere lettera morta. La certificazione non è un dettaglio: è ciò che consente di dimostrare la conformità, quando sarà richiesto.

Concludo. Più domande che risposte, certo. Ma il percorso da tracciare è chiaro: trasformare concetti come AI governance, AI compliance, AI responsabile, esplicabilità e fairness in pratica viva. La formazione, obbligatoria da febbraio 2025, non dev'essere una burocrazia inutile come certi crediti formativi per avvocati. Deve diventare terreno di cultura condivisa.

Dal 2 agosto 2026 la valutazione d'impatto sui diritti fondamentali sarà vincolante. La vera sfida non è la corsa alla compliance dell'ultimo minuto, ma la costruzione, fin da ora, di un equilibrio virtuoso tra innovazione e regolazione.

Come trovare questo equilibrio sostenibile? Non c'è una risposta unica. Ma so che la semplificazione secondo cui "più regole significa meno innovazione" non regge più. La regolazione può essere una bussola per l'innovazione responsabile. Se lo capiamo per tempo, se lo prendiamo sul serio, potremo rovesciare la narrativa. Non saremo più solo noi a inseguire modelli americani o asiatici. Ma sarà l'Europa, questa volta, a diventare laboratorio attrattivo di talenti e investimenti, grazie a un equilibrio intelligente tra innovazione e garanzie.