Da INSURANCE a *AI*NSURANCE - Gli effetti sul business e sull'offerta dell'accelerazione AI nelle Compagnie

Intervista a

Maddalena Rabitti - Consigliere IVASS

MF Festival delle Assicurazioni e della Previdenza - Insurance Day - *Nuovi rischi, nuove protezioni: come evolve il settore assicurativo tra IA, climate change e bisogni emergenti*

Milano, 6 ottobre 2026

1. **Negli ultimi mesi, anche grazie al dibattito promosso dagli operatori tecnologici più avanzati, si parla sempre più di sistemi di intelligenza artificiale che non si limitano a supportare l'uomo nelle analisi delle informazioni o nella formulazione di una decisione, ma agiscono come veri e propri agenti capaci di prendere decisioni e portarle a termine autonomamente. Se sistemi di questo tipo trovassero diffusione nei processi assicurativi, pensiamo ai processi di assunzione e valutazione dei rischi, di gestione dei rapporti con il cliente o di liquidazione dei sinistri, quali opportunità e quali criticità si potrebbero presentare per il settore (imprese, distributori, clienti)?"**

   Fino a poco tempo fa l'IA era principalmente uno strumento di supporto: aiutava a elaborare informazioni, formulare previsioni o suggerire possibili azioni. Oggi ci siamo avviati a una nuova fase, caratterizzata dalla diffusione di sistemi che non si limitano a suggerire, ma sono in grado di prendere decisioni e portarle a compimento, in modo autonomo.
   La vera discontinuità è quindi il passaggio dal supporto all'azione. Gli agenti IA possono raccogliere informazioni, interpretarle, prendere decisioni e avviare autonomamente attività conseguenti. Si tratta di un'evoluzione che può avere effetti molto significativi nel settore assicurativo.
   Ci saranno sicuramente applicazioni importanti. Pensiamo alla gestione dei sinistri. Potremmo avere sistemi capaci di acquisire documentazione, verificare le informazioni disponibili, stimare il danno, individuare anomalie e proporre o addirittura eseguire una liquidazione in tempi estremamente ridotti.
   Altri campi di applicazione promettenti sono la prevenzione delle frodi, l'assistenza alla clientela, la personalizzazione delle coperture.

In sintesi, il potenziale beneficio è rappresentato da maggiore efficienza, maggiore rapidità e maggiore capacità di adattare il prodotto alle esigenze del singolo cliente.
Ma ogni innovazione produce, accanto ai benefici, nuove responsabilità. Quanto maggiore è il grado di autonomia affidato ai sistemi, tanto più rilevante diventa il tema della governance.
Le questioni centrali riguardano la qualità dei dati utilizzati, l'affidabilità degli algoritmi, la robustezza dei controlli, la trasparenza delle decisioni e la possibilità di mantenere una supervisione umana effettiva.
L'assicurazione è un settore che si fonda sulla fiducia. Per questo motivo non è sufficiente che una decisione sia rapida o efficiente; deve essere anche comprensibile e trasparente.
Se un cliente riceve una proposta assicurativa oppure vede respinta una richiesta di indennizzo, deve poter comprendere le ragioni sottostanti e avere gli elementi per, eventualmente, contestare. Analogamente, l'impresa deve essere sempre in grado di spiegare il processo decisionale e assumersene la responsabilità.
Questo aspetto assume particolare rilevanza con l'introduzione di sistemi avanzati e progressivamente più complessi. Il rischio non è soltanto quello dei *bias* o degli errori di classificazione, temi ormai ben conosciuti. Emergono anche nuovi profili di rischio collegati al comportamento autonomo dei sistemi.
Alcuni episodi osservati negli ultimi mesi e ampiamente segnalati anche sui media mostrano che sistemi molto sofisticati possono perseguire un obiettivo assegnato in modi non sempre previsti dai progettisti, o addirittura perseguire un obiettivo non chiaramente assegnato. Ciò non significa necessariamente che diventino incontrollabili, ma evidenzia la necessità di rafforzare i meccanismi di supervisione.
Dal punto di vista della vigilanza il principio guida è molto chiaro: l'autonomia tecnologica non deve trasformarsi in una *delega opaca* della decisione e in una perdita di quella che possiamo definire "sovranità cognitiva".
Le imprese possono utilizzare strumenti sempre più avanzati, ma devono mantenere piena responsabilità delle scelte effettuate e la capacità di controllo sui processi. In IVASS abbiamo assunto, anche di recente, iniziative in tal senso.

2. **I danni causati dall'intelligenza artificiale sono assicurabili? Quali sono le principali criticità per il settore? L'intelligenza artificiale potrebbe diventare per il settore assicurativo quello che il cambiamento climatico è stato negli ultimi anni: un rischio sistemico difficile da misurare?**

Se in linea teorica il rischio derivante dall'utilizzo dell'IA è assicurabile, in linea pratica dobbiamo prima comprendere di cosa stiamo parlando.
Non si conosce ancora quale danno può essere generato, con quale gravità e livello di estensione, possiamo dire che siamo ancora nel terreno dell'ignoto perché non abbiamo serie storiche che ci consentono di tracciare un quadro, un perimetro del danno. I dati sono il primo indispensabile passo su cui l'assicurazione viene costruita.

Inoltre, non sappiamo ancora con sufficiente precisione come verrà distribuita la responsabilità tra sviluppatori, fornitori, utilizzatori e operatori che integrano tali sistemi nei propri processi, né quale potrà essere l'impatto di eventi che coinvolgano contemporaneamente migliaia o milioni di soggetti. Quanto più complessa diventa la filiera tecnologica, tanto più difficile può risultare individuare il soggetto effettivamente responsabile del danno.

In questo contesto assume rilievo il decreto legislativo n. 160 del 9 settembre 2026, che ha rafforzato gli strumenti di tutela del danneggiato e ha introdotto meccanismi destinati a favorire il risarcimento del danno cagionato da AI. Tra le nuove disposizioni, vi è anche la possibilità per il danneggiato di chiedere al presunto responsabile se ha una polizza a copertura del danno cagionato dall'AI e di agire in via diretta nei confronti dell'assicurazione.

Vi è poi un secondo aspetto da considerare che richiama, almeno in parte, il tema del cambiamento climatico. Naturalmente i due fenomeni sono profondamente diversi, ma condividono una caratteristica: la capacità di generare effetti correlati e potenzialmente sistemici. Ondate di calore, siccità, alluvioni e incendi boschivi tendono sempre più a verificarsi in modo concomitante o sequenziale, generando effetti cumulativi che mettono in discussione i tradizionali meccanismi di diversificazione del rischio su cui si fondano i modelli assicurativi e riassicurativi.

Con l'intelligenza artificiale potrebbe verificarsi qualcosa di analogo attraverso meccanismi differenti. Se migliaia di imprese utilizzassero gli stessi modelli, le stesse infrastrutture cloud o gli stessi fornitori tecnologici, un errore algoritmico, una vulnerabilità o un malfunzionamento potrebbe produrre danni simultanei e fortemente correlati. In questo senso l'IA potrebbe effettivamente assumere, per alcuni profili, caratteristiche tipiche di un rischio sistemico, perché aumenta il rischio di accumulazione e concentrazione delle esposizioni.

Vi è infine un ulteriore elemento. L'intelligenza artificiale non è soltanto un nuovo rischio da assicurare. È anche una tecnologia che modifica la natura di molti rischi già esistenti: pensiamo ai rischi operativi, cyber, professionali, reputazionali o di responsabilità civile. Questo rende più complessa la costruzione delle coperture e la determinazione dei premi.

Per questa ragione ritengo che la domanda corretta non sia tanto se l'intelligenza artificiale sia assicurabile, ma come creare le condizioni affinché lo diventi.

3. **È chiaro che sistemi di intelligenza artificiale avanzati possono avere implicazioni anche sull'integrità e sulla resilienza dei sistemi informatici delle imprese, anche quelle finanziarie, e sulla riservatezza delle informazioni. Proprio quest'estate IVASS ha chiesto alle compagnie assicurative di effettuare un *assesment* sui propri sistemi e di individuare e realizzare i necessari presidi di sicurezza e misure di protezione. Le imprese hanno tempo fino a fine anno per rispondere ad IVASS offrendo il quadro della situazione e dei rimedi. La Comunicazione di IVASS segnala la crescente attenzione delle autorità di vigilanza verso l'adozione dell'intelligenza artificiale avanzata nel settore finanziario. Che messaggio avete voluto dare alle imprese assicurative con questa Comunicazione? Che risposta vi aspettate**

dal mercato e soprattutto quali comportamenti o pratiche l'Autorità di vigilanza si aspetta che siano concretamente posti in essere?"

La comunicazione dell'IVASS in materia di resilienza operativa digitale e modelli avanzati di intelligenza artificiale recentemente pubblicata nasce da una considerazione semplice: negli ultimi anni abbiamo assistito a un'accelerazione senza precedenti delle capacità dei modelli di IA più avanzati.
Per questa ragione non è più possibile separare le riflessioni sull'IA da quelle sulla resilienza digitale, sul rischio operativo e sulla sicurezza informatica. Le tre dimensioni stanno progressivamente convergendo.
Un aspetto che preoccupa particolarmente riguarda la velocità. Storicamente le organizzazioni disponevano di un certo intervallo temporale per identificare una vulnerabilità, valutarne gli effetti e intervenire. Oggi questo margine tende a ridursi e la velocità con cui una vulnerabilità può essere individuata e sfruttata dagli attaccanti cresce rapidamente. Questo impone alle imprese di rafforzare la loro capacità di monitoraggio, prevenzione e risposta, e la velocità di ciascuno di questi processi.
Con la comunicazione IVASS abbiamo voluto invitare le imprese a una riflessione strutturata sul proprio livello di esposizione alle tecnologie di frontiera. Non si tratta di valutare soltanto dove e come viene utilizzata l'IA, ma anche quali siano le possibili conseguenze in termini di rischio operativo, cyber e di continuità aziendale.
Ci aspettiamo che le imprese rafforzino la governance, integrino questi rischi nei processi di risk management, aumentino l'attenzione verso i fornitori critici e sviluppino adeguate capacità di monitoraggio e risposta.
Il messaggio è semplice ma importante: non chiediamo di rallentare l'adozione delle nuove tecnologie bensì riteniamo fondamentale investire nella capacità di comprenderle, controllarle e presidiarle.
Da un punto di vista più ampio, oggi la resilienza non è più soltanto un fattore competitivo della singola impresa ma è un elemento essenziale della fiducia nel sistema finanziario nel suo complesso.
L'azione delle Autorità si muove pertanto lungo queste due dimensioni: monitoraggio e stimolo alle singole imprese affinché mettano i temi della resilienza digitale al centro della loro attenzione, e comprensione degli effetti dei nuovi sviluppi sulla stabilità dell'intero mercato assicurativo e finanziario.
Diversamente da quanto accaduto in altre stagioni dell'innovazione digitale, nelle quali la regolazione era spesso percepita come un ostacolo alla crescita, oggi anche una parte significativa dell'industria tecnologica riconosce apertamente la necessità di definire regole comuni e presìdi di sicurezza adeguati. Il punto centrale non è rallentare l'innovazione, ma evitare che la velocità del progresso tecnologico superi la capacità delle organizzazioni di comprenderne le implicazioni e di governarne i rischi.