INSURANCE Daily

N. 2976 GIOVEDÌ 9 APRILE 2026

PRIMO PIANO

I dati su Rc generale e Rc sanitaria

L'Ivass ha pubblicato un nuovo bollettino statistico dedicato ai rischi da responsabilità civile generale e Rc sanitaria, con i dati relativi al 2024.

Per quanto riguarda la Rc generale, la raccolta premi delle imprese vigilate dall'Ivass è stata di 4.157 milioni di euro (10,2% del totale danni), in crescita del 3,5% su base annua, e il costo medio dei sinistri è stato pari a 7.574 euro (+7,2% rispetto al 2023).

Per quanto riguarda il premio puro, che misura la sinistrosità del ramo, è risultato essere pari a 95,3 euro (+6,7% sul 2023). Il risultato del conto tecnico, al netto della riassicurazione, è positivo (871 milioni di euro), ma in calo del 23,1% sull'anno precedente soprattutto per l'incremento degli oneri per sinistri.

Relativamente alla Rc sanitaria, la raccolta premi in Italia nel 2024 è stata di 691 milioni di euro (-2,2% rispetto al 2023), soprattutto per la diminuzione della raccolta presso le strutture sanitarie pubbliche (-8,4%).

L'Ivass sottolinea come le strutture sanitarie pubbliche abbiano fatto "ampio ricorso alla ritenzione del rischio": nel 2024, gli accantonamenti ai fondi di ritenzione sono quasi il doppio dei premi pagati per coperture assicurative.

Alla fine del 2024 il mercato risultava assai concentrato: le prime dieci imprese hanno raccolto il 94,6% del totale dei premi; le prime cinque l'81,1%.

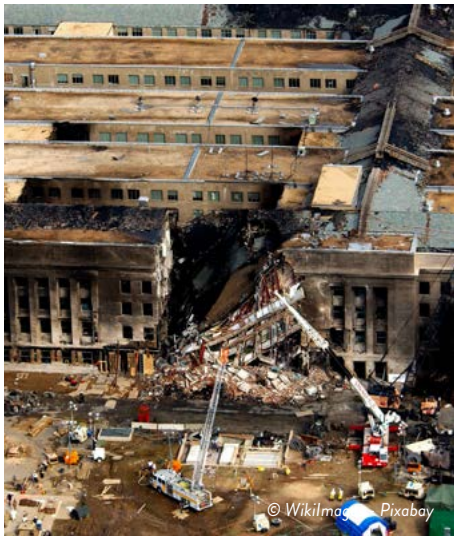
Il costo medio dei sinistri denunciati è stato di 38.341 euro, significativamente più elevato per le strutture pubbliche (83mila euro) rispetto alle strutture private (35mila euro) e al personale sanitario (20mila euro).

Beniamino Musto

RICERCHE

Terrorismo, rischio in evoluzione

La crescita dei conflitti a livello internazionale e delle tensioni sociali anche all'interno di singoli paesi aumenta la possibilità che si verifichino atti violenti contro infrastrutture, persone e proprietà. Il mercato assicurativo è chiamato a monitorare l'evolversi della minaccia e a proporre soluzioni adatte alle esigenze delle organizzazioni



Con il progressivo ritiro dei sistemi multilaterali, che per decenni hanno contribuito a conciliare le divergenze tra gli stati sui temi economici e politici, il rischio geopolitico e di conflitto è in evidente crescita. La percezione è diffusa, tanto che nell'ultimo *Global Risks Report 2026*, lo scontro geoeconomico è il rischio più citato (18%) tra le possibili cause di una crisi globale, seguito dal rischio di conflitti armati tra gli stati, terrorismo incluso (14%). A differenza della guerra, che rimane tendenzialmente confinata nelle aree direttamente interessate, il terrorismo assume una forma più subdola, nascosta e diffusa. Da questo punto di vista, è una minaccia che riguarda tutti i paesi, esprimendosi a volte in contesti apparentemente lontani dal focus della crisi, sia essa territoriale o ideologica.

Il modello di attacco terroristico che ha prodotto, uno su tutti, l'attentato dell'11 settembre 2001 a New York, costituito da reti terroristiche con una struttura gerarchica, è stato negli anni progressivamente sostituito da modelli più agili, formati da cellule decentralizzate che utilizzano il web come sistema di comunicazione, proselitismo, formazione e preparazione. In determinati casi, soprattutto se si tratta di terrorismo cyber, gli autori degli attacchi possono non essere guidati da un'ideologia e limitarsi a mettere a disposizione le proprie competenze. La svolta è anche metodologica: gli attacchi, fisici o digitali, sono studiati per massimizzare le conseguenze, sia in termini di vite umane che di danni materiali o di interruzione di attività, e non è esclusa la capacità di creare minacce nucleari o attacchi biologici, chimici e radiologici (Nbcr).

Il terrorismo assume forme che variano per metodi e origine: l'ideologia può portare all'assassinio di figure simboliche o a tentativi di stragi in luoghi affollati, per mano di singoli o di piccoli gruppi non necessariamente legati a forze politiche. C'è poi il terrorismo come arma di guerra, che colpisce fuori dall'area del conflitto per mettere in difficoltà il nemico (un esempio è il sabotaggio dei gasdotti Nord Stream). Sono in aumento i casi in cui l'instabilità interna di un paese ha ripercussioni al di fuori dei suoi confini; crescono le forme di radicalizzazione, alimentate da condizioni sociali ed economiche, così come aumentano le rivolte o le forme violente di risposta di fronte a tentativi di ridurre le libertà civili. L'evoluzione delle forme terroristiche o di rivolta, e il fatto stesso che non siano più attese solo nelle città ma ovunque sul territorio, sta modificando i metodi e i processi di identificazione delle minacce.

TRA PERCEZIONE E RISCHIO REALE

Il mutamento del quadro complessivo si riflette sul mercato assicurativo, con la necessità di adeguare l'offerta di protezione e la gestione del rischio. Il rapporto di **Marsh** *Global terrorism risk insurance report 2026* realizza una panoramica sul rischio terrorismo oggi e dedica spazio alle soluzioni assicurative, dalle forme di collaborazione pubblico-privato alle polizze *stand alone* specifiche.

Il mercato delle coperture contro gli atti terroristici è soggetto a una serie di fattori, primo dei quali è la percezione del rischio, maggiore in quelle realtà che, per posizione delle proprie strutture, sedi all'estero o attività che rientrano in obiettivi ideologici, possono ritenere di essere maggiormente esposte. Sul fronte opposto, una bassa percezione del rischio si incrocia comunque con le dinamiche di mercato nel momento in cui le condizioni delle assicurazioni property determinano nelle polizze all risk un aumento del costo anche delle garanzie sul terrorismo.


© Hubert de Thé - Pixabay

POLIZZE CYBER PER GLI ATTACCHI DAL WEB

Un aspetto emergente del rischio terroristico riguarda la minaccia cyber, che le potenzialità informatiche attuali rendono sempre più sofisticata e temibile. In questo contesto le strategie di mitigazione e le coperture specifiche possono offrire una valida protezione. L'ampia dipendenza dalle infrastrutture critiche, fisiche o digitali, costituisce un rischio sistemico a livello nazionale, in cui un singolo attacco potrebbe generare ripercussioni a cascata sull'intera economia. Il terrorismo cyber è una minaccia emergente e mutevole, e questo comporta due criticità molto sfidanti: innanzitutto, una scarsità di informazioni storiche utili alla modellizzazione del rischio, e poi la difficoltà di quantificare le potenziali perdite considerando le interdipendenze dei sistemi e la velocità di propagazione. Per fare fronte a questo rischio le polizze cyber possono tutelare le organizzazioni dalla perdita di dati, dai danni ai sistemi e dai rischi di interruzione dell'attività propria o della filiera.

PROTEZIONE SU MISURA PER CHI È PIÙ ESPOSTO

Le coperture terrorismo stand alone rappresentano una soluzione più flessibile e spesso innovativa per le organizzazioni che ricercano una protezione più efficace rispetto alle coperture standard. Anche se sottoscritte come garanzie integrative, consentono una personalizzazione dei termini di copertura, dei massimali e dei prezzi secondo i profili di rischio. Per le organizzazioni potenzialmente esposte, le polizze stand alone offrono una capacità più stabile anche in casi di escalation del rischio, inoltre consentono protezione da una gamma di minacce più ampia, laddove la definizione di "atto terroristico" in altri contesti di polizza può risultare riduttiva per le reali esigenze. Ulteriori vantaggi sono rappresentati dalla possibilità di estendere la protezione oltre i confini nazionali, di contare su massimali più elevati e di essere disponibili anche con contratti a lungo termine che garantiscono maggiore stabilità di prezzi e condizioni.

Le imprese più strutturate possono optare per coperture *captive*, a fronte di esposizioni elevate, per avere una soluzione personale e scegliere il rischio da trattenere e quello da trasferire. In questo senso, Marsh riferisce che negli Usa tra le compagnie captive che utilizzano i servizi di Marsh Captive Solutions sono state emesse, tra il 2023 e il 2024, 256 polizze a copertura di una o più linee di rischio previste dal *Tripra* (Terrorism risk insurance program reauthorization act) l'88% delle quali prevedeva almeno una garanzia specifica per il rischio terrorismo.

VALUTARE I PROGRAMMI NAZIONALI DI TUTELA

Al momento della scelta sulle coperture da attuare, è opportuno valutare l'ampiezza e i limiti di eventuali strumenti nazionali di protezione. Oltre agli Stati Uniti con il già citato Tripra, i governi di molti paesi hanno strutturato dei programmi di assicurazione per terrorismo che regolano i meccanismi di condivisione pubblico-privata del rischio, con coperture che in genere si attivano con il riconoscimento da parte del governo nazionale che un evento abbia avuto le caratteristiche dell'atto terroristico. Si tratta di modelli adattati agli spazi legislativi nazionali, con caratteristiche differenti ma in ogni caso attenti ad adeguare i termini di copertura all'evoluzione dei rischi. Il report di Marsh elenca infine pool riassicurativi in 23 paesi, di cui 10 in Europa (non in Italia), in buona parte attivati dopo il 2001.

Maria Moro

Per approfondire su www.insurancetrade.it:

- *Pool Re, un cat bond da 100 milioni di sterline*
- *Riassicurazione, non solo cat bond*

INSURANCE Daily

N. 2976 GIOVEDÌ 9 APRILE 2026

TECNOLOGIE

Come fare assicurazione nell'epoca dell'AI

Le compagnie sono davvero pronte a gestire i rischi connessi alla diffusione sempre più capillare dell'intelligenza artificiale? Se l'è chiesto Gallagher Re in un nuovo studio in cui analizza le offerte sul mercato, cercando di capire se le nuove minacce tecnologiche costituiscano o meno esposizioni inedite che richiedono prodotti dedicati

L'intelligenza artificiale si è diffusa più rapidamente della capacità del mercato assicurativo di assorbire i rischi generati. Questa la tesi di **Gallagher Re**, presentata nel suo nuovo report *Sistemi intelligenti, punti ciechi: ripensare le assicurazioni per l'era dell'AI*, che ha indagato in che modo le organizzazioni stanno integrando l'AI (generativa e non) nelle interazioni con i clienti, nei processi decisionali e nelle attività principali, e come potrebbero inconsapevolmente esporsi a una classe di responsabilità *native dell'AI* che le assicurazioni tradizionali potrebbero non riconoscere o non essere in grado di gestire al meglio.

Queste responsabilità, spiegano gli analisti della società che ha realizzato lo studio insieme a **Testudo**, non si manifestano necessariamente attraverso attacchi informatici, errori dei collaboratori o difetti nei prodotti, quanto da malfunzionamenti dei modelli di AI, e quindi allucinazioni, decisioni automatizzate errate, comportamenti discriminatori, modello e dati di addestramento corrotti. La giustizia e le autorità di regolamentazione spesso considerano questi problemi responsabilità di chi utilizza l'AI e non del fornitore della tecnologia. Del resto, le strutture contrattuali rafforzano questa percezione, grazie ai limiti di responsabilità del fornitore e indennizzi limitati che lasciano chi fa ricorso alla tecnologia esposto a rischi.

Quali polizze, per quali rischi

Diverse linee di business offrono una copertura per l'AI, ma permangono "lacune significative", scrivono gli analisti: "questa frammentazione crea incertezza – aggiungono nel report –, poiché le perdite legate all'AI possono far scattare diverse tipologie di assicurazione, a seconda degli *use case*, delle caratteristiche del sinistro e delle clausole della polizza". Ad esempio, un problema causato da un chatbot che interagisce con i clienti potrebbe innescare una richiesta di risarcimento per responsabilità civile; mentre un attacco informatico potrebbe attivare una polizza cyber. Altre polizze che potrebbero essere attivate da sinistri legati all'AI includono le polizze di responsabilità professionale in ambito tecnologico, Rc prodotti o Rc generale.

Il dibattito fondamentale, secondo Gallagher Re, verte sulla questione se i rischi legati all'intelligenza artificiale rappresentino sviluppi evolutivi all'interno delle coperture esistenti, cioè un'amplificazione dei rischi attuali, o costituiscano esposizioni completamente nuove che richiedono prodotti dedicati, in grado di affrontare i rischi derivanti dalla natura probabilistica di questa tecnologia.

Rc professionale in ambito tecnologico

Nelle polizze di cyber risk, per esempio, quando l'AI è il vettore dell'attacco, come il phishing basato sull'intelligenza artificiale o il deepfake, in genere si innesca la copertura, ma quando l'AI è la "fonte della responsabilità", cioè quando ci sono allucinazioni, discriminazioni, violazioni della proprietà intellettuale, generalmente la polizza non scatta.

Le polizze di responsabilità professionale in ambito tecnologico coprono i sinistri Rc verso terzi derivanti da servizi e prodotti tecnologici. Sebbene sia essenziale per gli sviluppatori e i fornitori di AI che vendono questi strumenti, non è in

genere rilevante per chi li utilizza, perché di fatto è un cliente e pertanto non è esposto al rischio che l'assicurazione è progettata per trasferire. Fondamentalmente, l'assicurazione di responsabilità professionale per il settore tecnologico tutela le organizzazioni che forniscono strumenti di intelligenza artificiale ad altri, non quelle che utilizzano intelligenza artificiale di terze parti: non copre lesioni personali, danni materiali, diffamazione, interruzione dell'attività, violazione della proprietà intellettuale, violazione del copyright, allucinazioni che causano perdite finanziarie o divulgazione di dati tramite output.

Servono modifiche alla Rc prodotti

Per quanto riguarda la polizza Rc prodotti, sostiene Gallagher Re, c'è da capire se il contratto sia adatto ai prodotti basati sull'intelligenza artificiale o se è l'intelligenza artificiale a poter essere considerata essa stessa un prodotto. Di recente, anche le aziende tecnologiche e di software sono diventate soggette a tale responsabilità, poiché il software è stato considerato un prodotto in diverse sentenze dei tribunali statunitensi, per esempio riguardo ad alcuni chatbot, e in alcune giurisdizioni, come la direttiva Ue sulla responsabilità del prodotto 2024/2853, entrata in vigore il 9 dicembre 2024 e che dovrà essere recepita dagli Stati membri entro il 9 dicembre di quest'anno.

Giacché i sistemi di intelligenza artificiale controllano sempre più dispositivi fisici (robot, veicoli autonomi e infrastrutture critiche), la Rc prodotti, argomentano gli analisti di Gallagher Re, potrebbe subire delle modifiche, a seconda che l'AI sia considerata un prodotto a sé stante o parte di un prodotto. Ad esempio, il Regno Unito ha una legislazione specifica (l'*Automated vehicles act 2024*) che considera la responsabilità per gli incidenti causati da veicoli autonomi come una responsabilità oggettiva del produttore.


© Gerd Altmann / Pixabay

Meglio una polizza stand alone o un'estensione?

Una limitazione fondamentale della responsabilità del prodotto è che si concentra sul danno fisico. I sinistri puramente algoritmici o di intelligenza artificiale, che causano perdite finanziarie o altri danni non fisici, non rientrano nell'ambito tradizionale della polizza, lasciando lacune sostanziali. La copertura, infine, esclude anche la violazione di brevetti, la diffamazione, le violazioni dei dati o della sicurezza, le perdite derivanti da deepfake e l'interruzione dell'attività. Si applica solo a produttori, fornitori e potenzialmente ad aziende tecnologiche e di software.

Al momento, scrive Gallagher Re nel report, il settore assicurativo sta rispondendo a queste e ad altre criticità attraverso due approcci complementari. In primis, le compagnie specializzate stanno sviluppando prodotti stand alone che coprono i rischi non adeguatamente considerati dalle polizze tradizionali; in secondo luogo, le imprese più importanti stanno introducendo clausole aggiuntive che adattano gli schemi di copertura esistenti. Entrambi gli approcci sono necessari per affrontare le sfide poste da questi nuovi rischi non assicurati.

La questione non è più stabilire se l'AI estenderà l'onere delle responsabilità, ma come il mercato assicurativo sarà in grado di adattarsi abbastanza rapidamente per affrontarle: le compagnie sono chiamate a costruire prodotti che riflettano i casi di fallimento effettivo dell'AI e i riassicuratori devono continuare a sviluppare le capacità adatte a esposizioni correlate e transfrontaliere", concludono gli analisti di Gallagher Re.

Fabrizio Aurilia

Per approfondire su www.insurancetrade.it:

- *Che cos'è davvero l'intelligenza artificiale per l'intermediazione assicurativa*
- *AI, investimenti a 500 milioni di euro nel 2028*

INSURANCE DAILY
Direttore responsabile: Maria Rosa Alaggio alaggio@insuranceconnect.it
Editore e redazione: Insurance Connect Srl – Via Montepulciano, 21 – 20124 Milano
T: 02.36768000 email: redazione@insuranceconnect.it
Per inserzioni pubblicitarie contattare: info@insuranceconnect.it
Supplemento al 9 aprile di www.insurancetrade.it – Reg. presso Tribunale di Milano, n. 46, 27/01/2012 – ISSN 2385-2577