INSURANCE Daily

N. 2975 MERCOLEDÌ 8 APRILE 2026

PRIMO PIANO

Universalità della Tun

La tanto attesa sentenza con cui la Cassazione era chiamata a pronunciarsi sull'applicabilità "generalizzata" dei criteri liquidativi stabiliti dalla Tun (Tabella unica nazionale) a tutti i danni non patrimoniali alla persona è stata pubblicata ieri (n. 8630/2026 del 7 aprile 2026) e ha confermato quanto molti si attendevano: la Tun, prevista dall'art. 138 del Codice delle assicurazioni e attuata dal Dpr 12/2025 in relazione al danno da invalidità comprese tra 10% e 100%, è applicabile anche agli eventi lesivi precedenti alla data della sua entrata in vigore (5 marzo 2025) e persino al di fuori dell'ambito oggettivo (Rc auto e Rc sanitaria) a cui l'art. 138 è esclusivamente dedicato.

Tale presa di posizione risponde alla questione interpretativa sollevata, mediante rinvio pregiudiziale ex articolo 363 bis del Codice di procedura civile, dal tribunale di Milano con l'ordinanza del 18 luglio 2025.

La questione, di grande impatto teorico e soprattutto pratico, mirava a comprendere se i giudici di merito potessero discostarsi dalle testuali indicazioni di legge, secondo le quali la Tabella unica nazionale avrebbe dovuto applicarsi ai soli sinistri della Rc auto e della Rc sanitaria verificatisi dopo il 5 marzo 2025, e utilizzarle anche nel calcolo della liquidazione relativa a sinistri danni accaduti in epoca precedente e relativi a fattispecie diverse.

Per leggere il resto della notizia, clicca qui.

Nei prossimi giorni, su Insurance Daily, sarà pubblicato un ampio approfondimento sui risvolti della sentenza.

Maurizio Hazan, Filippo Martini, Marco Rodolfi, *Studio legale THMR*

RISK MANAGEMENT

Trasporti, l'assicurazione passa (anche) dallo stretto di Hormuz

Gli eventi degli ultimi anni in Medio Oriente stanno ridisegnando la mappa del rischio guerra per il settore, modificando dinamiche consolidate. Fabrizio Frisoli, transport e cargo manager del broker Edge, teme che il comparto sia di fronte a una nuova normalità con la quale si dovrà convivere. Ma le soluzioni ci sono


© Alexander Kliem - Pixabay

Dal 28 febbraio scorso, il giorno dell'inizio della guerra mossa da Stati Uniti e Israele contro l'Iran, stiamo assistendo a una drammatica escalation e nemmeno il cessate il fuoco annunciato questa notte dal presidente americano Donald Trump sembra poter smuovere una situazione complicata, fatta di minacce, smentite, ultimatum e penultimatum. Abbiamo ormai imparato a memoria nuove toponomastiche: dall'isola di Kharg all'ormai onnipresente stretto di Hormuz, braccio di mare compreso tra l'Iran e i paesi del Golfo Persico la cui situazione sta causando una crisi energetica, dovuta alla scarsità di petrolio e gas.

Tuttavia, al netto della tragedia umana della guerra, il rischio di rotte interrotte con cui il trasporto marittimo deve fare i conti non è certo una situazione inedita: "si tratta di un contesto che, per certi versi, per gli addetti ai lavori è qualcosa di già visto", racconta a *Insurance Daily* **Fabrizio Frisoli**, transport e cargo manager del broker **Edge**. Basti ricordare ciò che era successo nel canale di Suez, quando la nave portacontainer *Ever Given*, della compagnia cinese **Evergreen**, si era incagliata il 23 marzo 2021, bloccando per sei giorni una delle rotte commerciali più importanti al mondo. Un blocco che aveva coinvolto oltre 400 navi, causando ritardi nelle catene di approvvigionamento globali. Oppure la crisi in Mar Rosso, quando nel 2023 gli Houthi dello Yemen hanno attaccato le navi occidentali che transitavano per quella rotta, cosa che, peraltro, si sta ripetendo in occasione di questa guerra.

NUOVE DINAMICHE NELLA SUPPLY CHAIN

"Già in passato – continua Frisoli – le merci hanno dovuto deviare il loro naturale *routing* in Medio Oriente. Oggi, per motivazioni diverse, è qualcosa che si sta ripetendo, cioè un routing modificato verso il sud del globo, con un passaggio dal capo di buona Speranza (Sudafrica, *ndr*) e tutta una serie di problematiche collegate al *transit time*, cioè al numero di giorni di viaggio, che, inevitabilmente, aumenta in modo significativo, così come aumentano i costi di trasporto, e soprattutto si delineano logiche e dinamiche diverse rispetto alla supply chain di un mercato ordinario".

Oltre al settore energetico, anche il comparto manifatturiero sta patendo queste criticità. "Nella logistica – spiega Frisoli – fatta eccezione per le navi che sono

tuttora bloccate nelle aree dove c'è la guerra, si sta già ragionando su come modificare i flussi anche attraverso rotte combinate (aereo e nave, *ndr*), piuttosto che utilizzare nuovi porti di trasbordo".

Il tema dei costi, invece, è molto complesso. Generalmente questi sono a carico del proprietario della merce ma in realtà ci sono diverse sfumature di cui gli addetti ai lavori devono tenere conto: ad esempio, chi fa il booking sulla nave o sull'aereo, chi risulta essere lo shipper ecc. "Potrebbero verificarsi situazioni in cui gli operatori logistici, essendo loro i primi soggetti che hanno fisicamente prenotato lo spazio a bordo delle navi, sono chiamati ad anticipare i maggiori costi", evidenzia Frisoli.


© Angad Cheema - Pixabay

L'IMPORTANZA DELLA FORZA NEGOZIALE

Ad aumentare l'incertezza, anche per gli assicuratori, c'è ovviamente il rischio guerra. Oggi, questo tema è decisamente più complesso, più ampio e anche poco prevedibile. "La sottoscrizione di questi rischi dipende più dalla geografia che dalla disciplina attuariale", osserva il manager di Edge. "Le variabili incidono sullo ship owner, la società armatoriale, perché l'equipaggio diventa un potenziale target da colpire".

Per coprire il rischio guerra, come noto, c'è stato un importante innalzamento dei prezzi, ma al momento la capacità assicurativa resta. "Da operatore del mercato – racconta Frisoli – confermo che la capacità c'è. Il pricing è sicuramente più elevato perché da un tasso standard rischio guerra allo 0,05% sul valore della merce, al netto di eventuali scontistiche commerciali o tecniche dovute a volume, dimensioni di business ecc., oggi si oscilla in un range tra lo 0,20% e lo 0,50%, quindi un costo che è diventato un moltiplicatore".

La crescita di Edge negli ultimi anni, agevolata dall'ingresso come primo azionista del fondo di private equity **AnaCap**, nel gennaio 2025, ha permesso alla società di avere una considerevole forza negoziale sul mercato: "noi stiamo parlando in virtù di una specialty che gestisce centinaia di polizze trasporti con partner con i quali lavoriamo quotidianamente e quindi non abbiamo difficoltà a reperire capacità presso le compagnie", spiega Frisoli. Detto ciò, il manager ovviamente non si esprime sul resto del settore: "non posso sapere – aggiunge – se un broker generalista che si trova a gestire una polizza trasporti, magari con un assicuratore che non è abituato a operare in questo ramo, riesca altrettanto facilmente a quotare questo rischio".

ASSICURARSI È LA PRIMA RISPOSTA

Gli eventi degli ultimi anni in Medio Oriente stanno ridisegnando la geografia del rischio guerra per il settore trasporti, modificando dinamiche consolidate. Frisoli, che non si spinge a fare previsioni, teme però che il comparto sia di fronte "a una nuova normalità con la quale si dovrà convivere". Nonostante ora ci si trovi in questa fase di stallo, in cui tanti operatori sono fermi in attesa che gli eventi evolvano, arriverà il momento in cui le decisioni andranno prese: "queste navi (all'ingresso dello stretto di Hormuz, *ndr*) non possono stare ferme lì per mesi perché i costi operativi stanno diventando molto rilevanti", precisa.

E quindi, quali sono le strategie che il broker consiglia alle aziende e agli operatori della logistica in tema di risk management? Frisoli rivela che, soprattutto all'inizio del conflitto, Edge ha ricevuto diverse telefonate da operatori che non sono clienti ma che chiedevano consulenza: "la risposta immediata è di assicurarsi contro il rischio guerra, che è quasi una certezza", dice il manager.

In Italia, solo il 30% delle merci è assicurato con una polizza trasporti, giacché come sappiamo la cultura assicurativa è bassa. L'auspicio, sottolinea il broker, è che, pur nella loro drammaticità, situazioni come quelle che sta vivendo il settore aumentino la cultura assicurativa: "gli operatori – conclude Frisoli – devono considerare l'assicurazione come se un asset strategico per la propria azienda, perché il mercato assicurativo sta facendo il proprio lavoro, ed è giusto riconoscergli il merito in queste situazioni di crisi".

Fabrizio Aurilia

Per approfondire su www.insurancetrade.it:

- *Hormuz, polizze per 40 miliardi di dollari*
- *Quanto costa assicurarsi per volare sul Golfo*

INSURANCE Daily

N. 2975 MERCOLEDÌ 8 APRILE 2026

RICERCHE

L'assicurabilità delle sanzioni cyber

Un report di Aon analizza come cambia l'esposizione delle imprese in seguito agli incidenti informatici, alla luce della crescente evoluzione normativa avvenuta in tutto il mondo (e in particolare in Europa), evidenziando l'importanza di comprendere le sfumature locali, la necessità di una stretta collaborazione tra le funzioni legali, di gestione del rischio e assicurative e di anticipare gli sviluppi normativi

Gli incidenti informatici si stanno diffondendo in ogni settore e a ogni latitudine, spingendo la corsa verso nuove normative volte a promuovere la resilienza, nonché a imporre multe e sanzioni a imprese, dirigenti e membri dei cda. In questo contesto, l'assicurazione cyber è un pilastro fondamentale della strategia di gestione del rischio informatico. Sebbene il suo obiettivo principale sia quello di fornire una protezione completa, è altrettanto importante comprenderne i limiti di copertura, ed è ciò che si propone di fare un report di **Aon** dal titolo eloquente, *The Insurability of Cyber Fines*, che indaga per l'appunto l'assicurabilità delle sanzioni informatiche.

Un cambio di scenario

Fino a poco tempo fa, gli obblighi normativi per le aziende colpite da incidenti informatici erano dettati principalmente dalle leggi sulla protezione dei dati, con alcune giurisdizioni che aggiungevano requisiti di resilienza operativa di portata limitata. Questo scenario è cambiato significativamente e continua a evolversi. L'Europa ha introdotto importanti quadri normativi come le direttive Dora e Nis2, così come anche il Regno Unito ha recentemente pubblicato il Cyber Security and Resilience Bill.

Secondo gli autori del report di Aon, si stanno delineando tendenze chiare. La prima riguarda il fatto che "le fonti delle sanzioni informatiche si sono ampliate considerevolmente". Oltre all'applicazione delle norme sulla protezione dei dati, un numero crescente di regolamenti specifici per il settore informatico "aumenta il rischio di sanzioni pecuniarie ingenti e introduce sanzioni non pecuniarie come il divieto di accesso ai dirigenti e la sospensione delle attività operative".

In secondo luogo, l'assicurabilità delle sanzioni informatiche rimane una questione incerta e specifica per ogni giurisdizione. Le leggi nazionali e le politiche pubbliche stabiliscono se tali sanzioni possono essere coperte da un'assicurazione, con alcuni paesi che impongono divieti generalizzati. Altri consentono l'assicurazione, salvo in caso di dolo o colpa grave.

Un terzo aspetto riguarda il fatto che l'applicazione delle norme sta diventando più incisiva. "Le autorità di regolamentazione – si legge nel report – non solo impongono sanzioni significative ma esaminano anche l'adeguatezza delle misure tecniche e organizzative, la tempestività della notifica delle violazioni e la solidità della risposta agli incidenti".

Assicurabilità delle sanzioni e limiti giuridici

Venendo all'aspetto centrale che dà il nome al report, cioè l'assicurabilità delle sanzioni cyber, lo studio ammette che questa è "una questione incerta e dipendente dalla giurisdizione", e che la possibilità di copertura vari da paese a paese. In alcuni ordinamenti esistono divieti generali, mentre in altri la copertura è ammessa con limitazioni. Il report precisa come alcuni paesi impongano divieti assoluti, mentre altri consentano l'assicurazione salvo nei casi di condotta dolosa o gravemente colposa, chiarendo il ruolo determinante del comportamento dell'assicurato.

Parallelamente, il report osserva come il mercato delle assicurazioni cyber abbia adottato un approccio flessibile alla copertura delle sanzioni, "laddove ciò sia legalmente consentito", adattandosi ai diversi contesti normativi.

Un ulteriore elemento riguarda la responsabilità individuale, giacché alcune giurisdizioni prevedono la responsabilità personale di amministratori e dirigenti, ampliando il perimetro del rischio oltre la sola impresa.

Il contenzioso continua ad aumentare

L'attività delle autorità di vigilanza si sta intensificando in modo significativo. Il report afferma che "l'azione di enforcement sta diventando più incisiva", indicando una maggiore propensione dei regolatori a intervenire. In particolare, è evidenziato come le autorità stiano aumentando il livello di controllo sugli aspetti tecnici e organizzativi "esaminando attentamente l'adeguatezza delle misure tecniche e organizzative, la tempestività delle notifiche di violazione e la solidità delle risposte agli incidenti", segnalando un'attenzione crescente alla gestione operativa del rischio.

Accanto all'enforcement regolatorio, si registra anche un incremento del contenzioso civile. Il report sottolinea che "l'emergere di meccanismi di azione collettiva e class action aggiunge un ulteriore livello di rischio legale", ampliando l'esposizione delle organizzazioni.

Questo contesto richiede un coordinamento tra diverse funzioni aziendali. Il report evidenzia "la necessità di una stretta collaborazione tra funzioni legali, di risk management e assicurative", sottolineando l'importanza di un approccio integrato.

Non è ancora chiaro come le normative di recente implementazione saranno applicate e se porteranno a un aumento sostanziale delle attività di contrasto. L'emergere di meccanismi di ricorso collettivo e di azioni collettive, in particolare a seguito dell'attuazione della direttiva Ue sulle azioni rappresentative (direttiva Ue 2020/1828), aggiunge un ulteriore livello di rischio di contenzioso. Le organizzazioni devono ora prevedere tanto le indagini normative quanto la possibilità di azioni collettive coordinate da parte di singoli individui e gruppi di consumatori.


© cottonbro studio - Pexels


© Lucas Andrade - Pexels

Uno sguardo al futuro

Guardando al futuro, Aon prevede che il contesto normativo diventerà "più esigente e dinamico". Gli standard di conformità probabilmente aumenteranno nel tempo, richiedendo un'attenzione costante e un adattamento da parte delle organizzazioni e dei loro leader. L'AI Act europeo, con i suoi rigorosi requisiti di sicurezza informatica per i sistemi di intelligenza artificiale ad alto rischio, e la possibilità di sanzioni cumulative, unitamente al Gdpr, è un esempio evidente di questa direzione. Le nuove normative attribuiscono maggiori oneri ai consigli di amministrazione e al management, con responsabilità diretta e maggiori aspettative in termini di supervisione e investimenti nella resilienza informatica.

In questo scenario, le organizzazioni sono chiamate a un aggiornamento costante. Il report sottolinea che "la conformità è un percorso continuo", evidenziando la necessità di un impegno costante per ridurre i rischi.

Infine, è necessario un rafforzamento delle responsabilità in capo ai vertici aziendali. Il report indica che "le nuove normative attribuiscono maggiori responsabilità ai consigli di amministrazione e al senior management", evidenziando un coinvolgimento sempre più diretto nella gestione del rischio cyber.

Beniamino Musto

Per approfondire su www.insurancetrade.it:

- *Furto di dati, cresce il pericolo di truffe più complesse*
- *Ecco come le imprese italiane fronteggiano i rischi informatici*

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 8 aprile di www.insurancetrade.it – Reg. presso Tribunale di Milano, n. 46, 27/01/2012 – ISSN 2385-2577