DAL MARE AL CIELO

di BENIAMINO MUSTO

INTERESSATI DA COSTANTI EVOLUZIONI TECNOLOGICHE E DA CONTINUI AGGIORNAMENTI NORMATIVI, I SETTORI TRASPORTI E AVIATION SONO DUE AMBITI MOLTO COMPLESSI SOTTO L'ASPETTO ASSICURATIVO PERCHÉ, PER LORO NATURA, AGISCONO NELLE DINAMICHE DI UNO SCENARIO INTERNAZIONALE IN CUI CI SONO MOLTEPLICI ELEMENTI DA TENERE IN CONSIDERAZIONE. UN WORKSHOP DELL'ANIA HA APPROFONDITO LE NOVITÀ PIÙ RILEVANTI EMERSE NELL'ULTIMO ANNO

Il workshop sui settori *Marine* e *Aviation*, organizzato ogni anno dall'**Ania**, rappresenta ormai un punto di riferimento per il settore, anche grazie al prezioso apporto di un panel di relatori sempre di alto livello. L'appuntamento di quest'anno, tenutosi il mese scorso via webinar, ha approfondito tematiche di grande attualità: le ripercussioni del caso Boeing e le problematiche connesse dei rischi aeroportuali, i rischi cyber per le navi e i veicoli a guida autonoma, e la nuova normativa europea che regolerà l'utilizzo dei droni in tutta Europa.

IL DIFETTO NEL SOFTWARE

A ottobre 2018, il volo JT 610 della LionAir precipitò al largo di Giacarta, facendo 189 vittime. A marzo 2019, il volo Ethiopian Airlines 302 si schiantò nei pressi di Bishoftu: persero la vita 157 persone. Sono due disastri aerei che riguardano modelli 737 Max della Boeing. Il modello coinvolto nei due incidenti è finito al centro di diverse indagini ed è stato fermato in diversi Paesi del mondo dopo le stragi. Dopo l'incidente l'**Easa**, Agenzia per la sicurezza del trasporto aereo dell'Unione europea, ha vietato il proprio spazio aereo ai Boeing 737 Max 8. Dalle indagini è emerso infatti che in entrambi i casi non c'è stato alcun errore umano ma un difetto di software del sistema anti-stallo Mcas. Un rapporto della Lion Air, citato da **Anna Masutti**, professoressa ordinaria di *Diritto della navigazione* presso l'Università di Bologna, ha identificato diversi fattori interconnessi: gravi errori sarebbero stati ravvisati nella certificazione di sicurezza, nell'addestramento dei piloti (impreparati a usare il software) e nei manuali degli aeromobili (carenza nella indicazione delle caratteristiche operative del software Mcas). Oltre alle richieste di risarcimento da parte dei familiari delle vittime, delle stesse compagnie aeree, e dei piloti, la Boieng ha subito perdite economiche dovute alla cancellazione degli ordini. Ma sono state mosse delle azioni anche da parte di Boeing nei confronti del produttore del software. Quest'ultimo, ha spiegato Masutti, è stato condannato a indennizzare più di 70 milioni di dollari: "un grande precedente, in assenza di una normativa che includa espressamene il software nella definizione di prodotto difettoso".


© volha84si - iStock

COSA CAMBIERÀ PER L'ASSUNZIONE DEI RISCHI

Il caso Boeing rappresenta il maggior sinistro assicurativo del settore a livello globale dai tempi dell'11 settembre, per danni, entità e numero di parti coinvolte.


© aapsky - iStock

Federica Bisetti, aviation underwriter di **Axa XL**, ha spiegato che l'impatto per Boeing da questo sinistro non riguarda solo gli indennizzi, ma anche le mancate commesse: si stima che solo nel 2019 l'azienda abbia perso all'incirca 630 milioni di dollari. Da marzo 2019 ben 350 aerei sono rimasti a terra, con circa 50 compagnie aeree coinvolte. E per una linea aerea, ha sottolineato Bisetti, "tener fermo un velivolo costa 150mila dollari al giorno". Secondo **Marcello Maestri**, aviation manager di **Aig**, sebbene gli indennizzi saranno assorbiti dai massimali, questi sinistri avranno una ripercussione negativa sui premi delle polizze: "il comparto assicurativo aeronautico – ha spiegato – era già in difficoltà da qualche tempo, e questi eventi hanno dato l'impulso a un aumento dei premi nei rinnovi. I premi raccolti dal settore aereonautico si sono rivelati, a livello globale, insufficienti a coprire i sinistri generati negli ultimi anni". Secondo Federica Bisetti, inoltre, la spinta a ridurre emissioni e consumi porterà nel breve e nel medio termine a delle evoluzioni nella tecnologia degli aereomobili. "Nel futuro – ha osservato – ci saranno delle rivoluzioni, e questo andrà a

REGOLE IN EVOLUZIONE PER I DRONI

La regolamentazione riguardante i droni è in continua evoluzione, e per questo è stato deciso di dedicarvi una specifica sessione del seminario organizzato dall'Ania. **Alessandro Sabatini**, l'aviation underwriter di **Satec**, ha ripercorso le tappe a partire dal 2012, con le prime richieste di coperture per droni; del 2013-2014 la prima edizione del regolamento **Enac**. Nel 2016-2017 c'è stata un'espansione della domanda, in seguito alla quale gli assicuratori hanno iniziato a ragionare su una sorta di standardizzazione che ha portato, nel 2018, a nuovi metodi assuntivi. "Gli operatori abilitati sono aumentati del 350% dal 2016 al 2019, e si stima che attualmente in Italia ci siano più di 13mila droni attivi", ha detto. A scendere poi nei dettagli degli aspetti normativi, è stato l'ingegner **Sebastiano Veccia** direttore regolazione personale e operazioni volo dell'Enac, che ha parlato degli obblighi assicurativi in riferimento al nuovo regolamento europeo **Easa** del 2019, la cui introduzione, prevista per luglio, slitterà al prossimo anno. Nell'attesa resta in vigore in Italia il terzo regolamento Enav, che ha introdotto il rilascio del patentino (per i mezzi più semplici, quelli fino a 25 kg) previo superamento di una prova online. "Rilasciamo una media di 250 attestati al giorno – ha spiegato – e dal 5 marzo scorso abbiamo rilasciato circa 15mila attestati". Per quanto riguarda l'aspetto assicurativo la differenza sostanziale introdotta dal Regolamento 3 è che il mezzo deve essere obbligatoriamente assicurato per la responsabilità civile. Una norma destinata a durare, visto che "il regolamento europeo dice che per gli aspetti assicurativi possono applicarsi le regole dello Stato membro", ha ricordato.

impattare sulla filiera, inclusa l'assicurazione. Le nuove tecnologie inoltre non potranno contare su statistiche pregresse, quindi ci sarà una maggiore esposizione, così come aumenterà anche il rischio cyber".

LA MINACCIA CYBER VIAGGIA SUI MARI

Quella dei rischi cyber è una minaccia che già incombe nell'ambito dei trasporti marittimi. L'avvocato **Claudio Perrella**, partner dello studio legale **R&P Legal**, ha ripercorso le tappe con cui il mercato assicurativo ha provato a fare ordine in una materia molto intricata perché estremamente mutevole. La Pra (Prudential regulation authority) britannica, ha riferito Perrella, "ha esortato il mercato a intervenire, e a partire dal luglio 2019 c'è stata un'elaborazione di clausole". In un contesto nel quale non è più soltanto il conducente a decidere ma anche l'intelligenza artificiale, ci sono diversi risvolti etici, quindi la tendenza futura vedrà sempre più "una responsabilità di prodotto in relazione a chi progetta il software, e sarà una responsabilità non più presunta, come ora, ma oggettiva", ha concluso l'avvocato. Con l'applicazione dell'intelligenza artificiale allo shipping cambiano i concetti di nave, comandante, equipaggio, navigabilità: "dal punto di vista assicurativo – ha detto **Roberto Spanu** – senior risk engineer marine di **Swiss Re Corporate Solutions** – bisognerà capire come coprire errori di programmazione o perdita di connettività dei dati".


© AvigatorPhotographer - iStock

LE SMART SHIPS SONO GIÀ REALTÀ

Il mercato connesso alle navi autonome è stato stimato intorno agli 88 miliardi di dollari per il 2020, e potrebbe sfiorare i 135 miliardi di dollari nel 2030. "A oggi – ha proseguito Spanu – non esiste una definizione di cosa sia una nave autonoma, e quali siano i diversi livelli di autonomia applicati, e quindi i rischi di eventi cyber associati". Spanu ha spiegato che le smart ships sono già realtà, e sistemi di bordo IoT sono sempre più presenti. Sono già in esercizio navi che a prima vista possono essere definite *tradizionali*, ma i cui sottosistemi sono collegati tra loro e controllati h24 da sistemi di monitoraggio a terra. "Tutti potenziali punti di ingresso per attacchi hacker o incidenti cyber", ha aggiunto l'esperto, ricordando che "ci sono già stati casi di incidenti legati a attacchi cibernetici, e in futuro saranno potenzialmente favoriti dalla maggiore interconnessione dei sistemi". Secondo alcune analisi i maggiori danni potrebbero però esserci non tanto alla nave o al carico, ma alla struttura, come ad esempio una piattaforma petrolifera. "La minaccia – ha concluso Spanu – non si limiterà al solo funzionamento della nave, ma a tutto l'ecosistema. C'è molto da fare per migliorare la resilienza, perché gli eventi legati alla sicurezza informatica non sono statici, quindi anche le difese vanno costantemente aggiornate".