



La cybersecurity nel trasporto aereo: le recenti normative europee e internazionali

Doriano Ricciutelli*

Lo scorso 17 gennaio è entrata in vigore la Direttiva UE/2555/2022 del 14 dicembre 2022 (c.d. direttiva NIS 2), che dovrà essere recepita dagli Stati membri nei rispettivi ordinamenti interni.

Nel panorama delle novità rispetto alla precedente, abrogata, direttiva UE 2016/1148 (NIS 1) rilevano, *inter alia*, le disposizioni sulle misure di gestione dei rischi di cybersecurity di cui all'art. 21. In particolare, si prevede che gli Stati membri, oltre ad un determinato obbligo di segnalazione stabilito dall'art. 23, debbano provvedere affinché i "soggetti essenziali e importanti" adottino misure tecniche, operative e organizzative adeguate e proporzionate per gestire i rischi posti alla sicurezza dei sistemi informatici e di rete utilizzati da questi soggetti nelle loro attività, nonché per prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei loro servizi.

Anche in ragione della normativa europea e internazionale di settore, e considerando i rispettivi costi di attuazione, le predette misure dovranno assicurare un livello di sicurezza dei sistemi informatici e di rete adeguato ai rischi esistenti. Riveste, quindi, un ruolo di assoluta importanza la valutazione della proporzionalità di tali misure, rispetto alla quale risulta opportuno tener debitamente conto del "grado di esposizione del soggetto a rischi, delle dimensioni del soggetto e della probabilità che si verifichino incidenti, nonché della loro gravità, compreso il loro impatto sociale ed economico" (art. 21, comma 1, direttiva (UE) 2555/2022).

Giova ancora rappresentare che, per quanto concerne l'ambito applicativo della novella in materia di aviazione civile, contemplato nell'allegato I della direttiva *de qua* si individuano, quali settori "ad alta criticità", i vettori aerei come definiti all'articolo 3, punto 4), del regolamento (CE) n. 300/2008 utilizzati a fini commerciali, i gestori aeroportuali individuati dall'articolo 2, punto 2), della direttiva 2009/12/CE del Parlamento europeo e del Consiglio, aeroporti quali definiti all'articolo 2, punto 1), di tale direttiva, compresi gli aeroporti centrali di cui all'allegato II, sezione 2, del regolamento (UE) n. 1315/2013 del Parlamento europeo e del Consiglio, e soggetti che gestiscono impianti annessi situati in aeroporti nonché, infine, gli operatori attivi nel controllo della gestione del traffico che fornisco-

no un servizio di controllo del traffico aereo quali definiti all'articolo 2, punto 1), del regolamento (CE) n. 549/2004 del Parlamento europeo e del Consiglio". Pertanto, attraverso il richiamo al citato regolamento di base n. 300 il pacchetto della "cybersicurezza" dell'Unione si innesta nel quadro della security dell'aviazione civile, peraltro recentemente ricompreso nella disciplina del regolamento della Commissione UE/1583/2019 la cui implementazione è costantemente monitorata dall'apposito comitato AVSEC (DOC 11301 del marzo 2023) e dall'Aviation Cybersecurity Working Group (3° meeting del 22 novembre 2022). Quest'ultimo provvedimento di esecuzione detta, infatti, in nome di una necessitata partnership tra enti pubblici e privati, norme che impongono alle autorità competenti di stabilire e attuare procedure per la condivisione delle informazioni pertinenti di ausilio ad altre autorità e agenzie nazionali, agli operatori aeroportuali, ai vettori aerei e ad altri soggetti interessati, di modo che possano eseguire efficaci valutazioni dei rischi per la sicurezza in relazione alle loro operazioni. Inoltre, si introducono precetti sulla individuazione dei dati e dei sistemi di tecnologia dell'informazione e della comunicazione fondamentali per l'aviazione civile e le loro protezioni dalle minacce informatiche.

Sul piano internazionale la 41° Assemblea dell'ICAO ha pubblicato, con il Doc. 1084, le ultime risoluzioni in vigore a decorrere dal 7 ottobre 2022 e, segnatamente, nella parte VII dedicata al capitolo sulla "Unlawful interference" viene dedicato uno specifico spazio al tema "Addressing Cybersecurity in Civil Aviation". Se da un lato l'assemblea esorta gli Stati membri dell'organizzazione ad adottare e ratificare la Convenzione di Pechino per la repressione degli atti illeciti contro l'Aviazione civile internazionale e il Protocollo addizionale alla Convenzione per la soppressione del sequestro illegale di aeromobili come mezzo per affrontare gli attacchi informatici contro il trasporto aereo, dall'altro, invita gli Stati e le parti interessate del comparto a intraprendere una serie di azioni significative per affrontare la minaccia cyber nel novero delle quali assume rilievo l'implementazione la strategia dell'ICAO per la cybersicurezza dell'aviazione e l'utilizzo coerente del relativo piano d'azione.

* Docente universitario a contratto