La recente normativa europea per una aviazione civile cyber resiliente

Doriano Ricciutelli*

Il 2 febbraio 2023 la Commissione europea ha pubblicato il regolamento di esecuzione 203/UE/ 2023 completando il quadro normativo aperto a un meccanismo di aviazione cyber-resiliente la cui fonte primaria risiede nell'impianto introdotto dal regolamento 1139/UE/2018.

In particolare, l'atto dell'esecutivo comunitario stabilisce numerose norme finalizzate a identificare e gestire i rischi per la sicurezza delle informazioni nell'ambito delle organizzazioni aeronautiche e delle autorità responsabili in materia di aviazione, inclusa l'Agenzia dell'Unione Europea per la sicurezza dell'Aviazione Civile (EASA), seguendo coerentemente la disciplina del regolamento delegato 1645/UE/2022 del 23 settembre 2022, applicabile agli enti approvati di progettazione e produzione, nonché ai gestori aeroportuali e agli erogatori di servizi (*handler*) nel piazzale degli aeromobili (*apron*).

Infatti, per inciso, il ruolo dell'EASA sta nel garantire che i rischi informatici siano presi in debita considerazione durante la realizzazione , lo sviluppo e l'esercizio degli aeromobili - come si evince dal documento dell'agenzia stessa "*The European plan for Aviation Safety (EPAS 2021-2025) RMT.0720*" - ed è incentrato nel sostenere energicamente la crescita di un sistema aereo europeo sicuro, operando attraverso la promozione, la regolamentazione e la cooperazione internazionale per incorporare la cyber security nel concetto della esistente "*aviation security*".

Ciò premesso, a ben vedere, il regolamento n. 203 prevede elementi funzionali per il rilevamento degli eventi che potrebbero pregiudizievolmente influire sui sistemi di tecnologia dell'informazione e della comunicazione e sui dati utilizzati per gli scopi dell'aviazione civile, introducendo, nel contempo, i requisiti necessari alla "*risposta*" e al "*ripristino*", a seguito di incidenti cyber, a un livello commisurato al relativo impatto sulla security aerea ed aeroportuale.

Secondo quanto sancito dall'art. 3 del regolamento in questione riguardante le "definizioni", osserviamo che per «*sicurezza delle informazioni*» si debba intendere "*la tutela della riservatezza, dell'integrità, dell'autenticità e della disponibilità della rete e dei sistemi informativi*".

Al riguardo, lo stesso regolamento (considerando 12) sostiene che la lettura della predetta espressione, capace di riflettere il suo uso comune nell'aviazione civile sul piano globale, debba risultare analoga a quella dei termini «*sicurezza della rete e dei sistemi informativi*» fissati dall'articolo 4, punto 2, della direttiva 1148/UE/2016" (direttiva NIS 1) e non essere "*interpretata in modo divergente*" dalla accezione da essa descritta.

Orbene, alla luce del combinato disposto dell'art. 44 e della "*tavola di concordanza*" contenuta all'allegato III della direttiva 2555/UE/2022, la suindicata interpretazione va ricercata nel dettato dell'articolo 6 di quest'ultima novella (direttiva NIS 2, abrogativa della precedente) in cui la locuzione- peraltro lievemente trasformata- «*sicurezza dei sistemi informatici e di rete*» viene più estesamente declinata, aggirando l'impasse, con il significato giustappunto di "*capacità dei sistemi informatici e di rete di resistere, con un determinato livello di confidenza, agli eventi che potrebbero compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o elaborati o dei servizi offerti da tali sistemi informatici e di rete o accessibili attraverso di essi*".

Conviene, comunque, evidenziare in proposito che il suesposto assunto ermeneutico riveste un interesse non trascurabile, rispetto anche a taluni profili del campo assicurativo, ove si consideri, a mero titolo esemplificativo, che nei recenti "*Orientamenti sulla Sicurezza e sulla Governance dell'ICT*" dell'EIOPA, operativi dal 1 luglio 2021, sembrano rilevare certi essenziali aspetti definitori afferenti, inter alia, proprio ai rischi per la "sicurezza delle informazioni" (es. transazioni dei fornitori, minacce informatiche, incidenti di *Information and Communication Technologies*, ecc.).

Del resto preme denotare che nel regolamento n. 203 è altresì presente una serie di ulteriori richiami a disposizioni appartenenti alla oramai superata direttiva NIS 1 che, evidentemente, in base alla prefata tavola sono automaticamente allineati alle analoghe norme della direttiva n. 2555.

Nel novero di questi riferimenti annotiamo gli "*obblighi*" di sicurezza delle informazioni e di cyber sicurezza, la nozione di "*inconveniente*" poi espunta radicalmente dal lessico dei successivi articolati, il tema connesso agli "*orientamenti*" per le valutazioni di competenza della Commissione circa l'"*equivalenza*" tra i requisiti indicati dalla direttiva NIS 1 e dal regolamento n. 203 e, da ultimo, le pertinenti "*comunicazioni*" delle autorità competenti al "*punto di contatto unico designato*".

In ordine alla correlazione con il sistema della security dell'aviazione civile, riscontriamo, infine, la previsione alquanto significativa secondo la quale, nel caso un'organizzazione (impresa) sia un'entità di cui ai programmi nazionali prescritti a norma dell'articolo 10 del regolamento 300/CE/2008 (vettori aerei, operatori e altri soggetti aeroportuali), i succitati obblighi di cyber sicurezza, descritti al punto 1.7 dell'allegato del regolamento di esecuzione 1998/UE/2015 (ult. mod. regolamento 566/UE/2023 del 10/3/2023), sono considerati equivalenti ai requisiti imposti dal regolamento n. 203, tranne per quanto riguarda il punto IS.I.OR.230, "*che è da rispettare di per sé*" e concerne il "*sistema di segnalazione esterna della sicurezza delle informazioni*".

* Docente universitario a contratto