

SICUREZZA DEI DRONI E ANTIDRONE: IL PIANO D'AZIONE COM(2026) 81

Nicola Romana *

SOMMARIO: 1. Premessa – 2. Natura dell'atto e geometria delle competenze – 3. Prevenzione: il *Drone Security Package* e la revisione dei regolamenti 2019/945 e 2019/947 – 4. Infrastrutture critiche, frontiere, spazi marittimi e sicurezza dei prodotti – 5. Rilevamento: dati, reti di telecomunicazione e spettro – 6. Risposta: il nodo dei poteri di neutralizzazione – 7. La dimensione della difesa e la svolta securitaria – 8. Valutazione e conclusioni.

1. – L'11 febbraio 2026 la Commissione ha adottato il Piano d'azione sulla sicurezza dei droni e antidrone ¹. L'atto risponde alle sollecitazioni del Consiglio europeo del 23 ottobre 2025 e a due risoluzioni del Parlamento europeo, del 9 ottobre 2025 e del 22 gennaio 2026, approvate a fronte di una serie di sorvoli ostili, violazioni dello spazio aereo e chiusure di aeroporti che hanno interessato diversi Stati membri a partire dal settembre 2025 ².

Il contesto spiega il registro del documento. Il Piano descrive una minaccia che va dalla negligenza del singolo operatore alle operazioni ibride di attori statali, e che si estende dallo spazio aereo alle infrastrutture energetiche, ai porti, alle frontiere esterne e agli spazi pubblici. Rispetto alla Strategia per i droni 2.0, la sicurezza non compare più come condizione per lo sviluppo del merca-

* Università degli studi di Palermo.

Il contributo tiene conto delle fonti disponibili al 19 ottobre 2026.

¹ Comunicazione della Commissione al Parlamento europeo e al Consiglio, *Piano d'azione sulla sicurezza dei droni e antidrone*, COM(2026) 81 final, 11 febbraio 2026, in <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52026DC0081>; testo trasmesso al Consiglio come doc. 6262/26, in <https://data.consilium.europa.eu/doc/document/ST-6262-2026-INIT/en/pdf>. Presentazione sintetica sul sito della Commissione: Action Plan on Drone and Counter Drone Security, ultimo aggiornamento 12 febbraio 2026, in <https://digital-strategy.ec.europa.eu/en/policies/drone-security>.

² Conclusioni del Consiglio europeo del 23 ottobre 2025, EUCO 18/25; risoluzione del Parlamento europeo del 9 ottobre 2025 su una risposta unitaria alle recenti violazioni russe dello spazio aereo e delle infrastrutture critiche degli Stati membri (2025/2901(RSP)); risoluzione del Parlamento europeo del 22 gennaio 2026 sui droni e i nuovi sistemi di guerra (2025/2088(INI)). Riferimenti tratti dalle note 1 e 2 del Piano.



to, ma come obiettivo autonomo, al quale lo sviluppo del mercato viene a sua volta collegato: un mercato affidabile, si legge, presuppone che i droni legittimi non possano essere trasformati in vettori di minaccia.

La tesi di queste pagine è che il Piano sposti il baricentro della disciplina europea dei droni dal paradigma della *safety* a quello della *security*³, non perché la *security* vi compaia per la prima volta, ma perché, nelle nuove iniziative regolatorie, da finalità concorrente diventa finalità prevalente, e che lo faccia seguendo nel complesso la mappa delle competenze dell'Unione, pur forzandone talvolta i confini. Dove l'Unione dispone già di una base giuridica settoriale (sicurezza aerea, mercato interno dei prodotti, spettro radio), il Piano annuncia atti vincolanti a breve termine. Dove prevalgono le competenze e le responsabilità operative degli Stati membri (sicurezza nazionale, ordine pubblico, protezione fisica delle infrastrutture), il Piano propone strumenti volontari, raccomandazioni e meccanismi di coordinamento. Il nodo che sta tra i due ambiti, cioè chi possa legittimamente neutralizzare un drone e a quali condizioni, è affidato a uno studio di fattibilità con orizzonte al 2030.

Il passaggio non è neutro, e desta preoccupazione. La *safety* aeronautica aveva una misura interna: la proporzionalità rispetto al rischio operativo, per

³ Sulla distinzione tra *safety*, intesa come prevenzione degli eventi accidentali connessi all'esercizio della navigazione, e *security*, intesa come protezione contro gli atti di interferenza illecita, e sulle loro interrelazioni, v., senza pretesa di completezza, M.M. Comenale Pinto, *I profili di security e le interrelazioni con le normative di safety*, in G. Camarda, M. Cottone, M. Migliarotti (a cura di), *La sicurezza negli aeroporti. Problematiche giuridiche ed interdisciplinari*, Milano, 2005, p. 53 ss., anche in *Dirittoestoria*, n. 3, 2004, in <https://www.dirittoestoria.it/3/Lavori-in-Corso/Contributi/Contributi-web/Comenale-Security.htm>, che le definisce «due facce della medesima moneta»; F. Pellegrino, *Sicurezza e prevenzione degli incidenti aeronautici nella normativa internazionale, comunitaria e interna*, Milano, 2007; G. Camarda, *La sicurezza nel diritto della navigazione*, in U. La Torre, A.L.M. Sia (a cura di), *La sicurezza nel trasporto e nelle infrastrutture della navigazione marittima ed aerea*, Soveria Mannelli, 2011, p. 11 ss.; A. Antonini, *La sicurezza in campo aeronautico*, ivi, p. 267 ss.; F. Pellegrino, *Le competenze del gestore aeroportuale nel quadro della safety e della security dell'aviazione civile*, in S. Busti, E. Signorini, G.R. Simoncini (a cura di), *L'impresa aeroportuale a dieci anni dalla riforma del codice della navigazione: stato dell'arte*, Torino, 2016, p. 63 ss.; C. Severoni, *La sicurezza dell'aviazione civile e i limiti alla libertà di circolazione: riflessioni a seguito della pandemia da COVID-19*, in *Riv. it. dir. tur.*, 2020, n. speciale, p. 149 ss.; E. Sena, *Sicurezza della navigazione aerea e tutela del lavoro del personale di volo*, Torino, 2023, spec. p. 4 s.; per la navigazione marittima, C. Telesca, *I rischi concernenti la sicurezza (security e safety) e la loro assicurabilità*, Bari, 2024, p. 1 ss. Nella letteratura internazionale, J. Huang, *Aviation Safety through the Rule of Law: ICAO's Mechanisms and Practices*, Alphen aan den Rijn, 2009; R. Abeyratne, *Aviation Security Law*, Berlin-Heidelberg, 2010. Per gli aeromobili senza equipaggio, v. *infra*, note 4, 6 e 9.

cui gli obblighi crescono con la pericolosità dell'operazione. La *security* comporta invece una valutazione delle minacce intenzionali con margini di incertezza e di discrezionalità più ampi, e non ha una misura interna altrettanto definita: i suoi limiti le vengono soprattutto dall'esterno, dai principi che condizionano ogni restrizione dei diritti fondamentali, cioè la previsione per legge, la necessità e la proporzionalità (art. 52, par. 1, della Carta dei diritti fondamentali dell'Unione europea). Sono limiti più difficili da far valere quando la minaccia, per definizione, può sempre giustificare un passo ulteriore. Quando la *security* diventa il principio ordinatore di una disciplina nata per rendere sicuro e accessibile l'uso civile dello spazio aereo, il rischio è che assorba gli altri valori in gioco, dalla libertà d'impresa al rispetto della vita privata e alla protezione dei dati personali (artt. 16, 7 e 8 della Carta). Il Piano, come si vedrà (§ 7), si inserisce in una più ampia svolta securitaria della politica della Commissione, che investe sempre più anche la difesa.

Per il diritto dei trasporti il Piano interessa sotto tre profili: la revisione del quadro regolatorio degli aeromobili senza equipaggio; la protezione di aeroporti, porti e nodi di trasporto, che il Piano tratta come infrastrutture critiche senza però raccordarsi con la disciplina della *security* aeroportuale e portuale; la ripartizione tra soggetti pubblici e gestori privati, spesso concessionari, degli oneri di rilevamento e di risposta.

2. – Il Piano è una comunicazione al Parlamento europeo e al Consiglio e non produce effetti vincolanti. Lo dice esso stesso nelle conclusioni, qualificando le azioni come proposte agli Stati membri fondate sul principio di «co-ownership» e annunciando una discussione strutturata con Stati, industria e Parlamento per stabilirne le priorità. La sua forza dipende quindi dagli atti che ne discenderanno, dalle risorse finanziarie mobilitate e dal meccanismo di governance: un coordinamento strategico con gli Stati membri, un coordinatore nazionale per la sicurezza dei droni in ciascuno Stato e un rapporto annuale di monitoraggio basato su contributi volontari.

Sul piano sistematico, il Piano si colloca accanto alla *Strategia per i droni 2.0* del 2022, che resta il quadro generale per lo sviluppo del mercato, e sostituisce la revisione intermedia della comunicazione del 2023 sul contrasto alle minacce dei droni ⁴. Rispetto a quest'ultima, che riguardava i soli droni civili usati in mo-

⁴ Comunicazione della Commissione, *Strategia per i droni 2.0*, COM(2022) 652 final; comu-

do illecito, l'oggetto si allarga in due direzioni: ai droni terrestri, di superficie e subacquei, oltre che ai palloni meteorologici usati per il contrabbando; e alla dimensione della difesa, con cui il Piano intende realizzare sinergie civili-militari.

La premessa competenziale è dichiarata con chiarezza: la protezione delle infrastrutture critiche, delle frontiere e degli spazi pubblici e la sicurezza aerea e marittima restano in primo luogo di competenza degli Stati membri, mentre il carattere transfrontaliero degli incidenti giustifica coordinamento e solidarietà a livello europeo. La formula riecheggia l'art. 4, par. 2, TUE, secondo cui la sicurezza nazionale resta di competenza esclusiva di ciascuno Stato membro, e l'art. 72 TFUE, che nello spazio di libertà, sicurezza e giustizia fa salve le responsabilità degli Stati per il mantenimento dell'ordine pubblico e la salvaguardia della sicurezza interna. Il richiamo va però inteso con precisione: queste disposizioni riservano agli Stati la responsabilità ultima della sicurezza e l'esercizio operativo della forza, non sottraggono all'Unione i settori interessati, nei quali essa dispone di competenze proprie, a cominciare dalla sicurezza aerea e marittima. La conseguenza è che il Piano non si fonda su una base giuridica unitaria, ma mobilita titoli diversi: la politica dei trasporti (art. 100, par. 2, TFUE), su cui poggia il regolamento (UE) 2018/1139; il ravvicinamento delle legislazioni (art. 114 TFUE), base del regolamento sulla ciberresilienza e della direttiva sulla resilienza dei soggetti critici; la gestione delle frontiere esterne; i programmi industriali e di difesa. In dottrina si è parlato, a questo proposito, di una «ibridazione» di competenze e strumenti, nella quale l'Unione usa titoli funzionali al mercato interno per incidere su ambiti tradizionalmente riservati agli Stati ⁵.

nicazione della Commissione sul contrasto alle potenziali minacce poste dai droni, COM(2023) 659 final. Sul quadro europeo e internazionale degli aeromobili senza equipaggio, B.I. Scott (a cura di), *The Law of Unmanned Aircraft Systems*, 2ª ed., Alphen aan den Rijn, 2022 (Aerospace Law and Policy Series, vol. 11); A. Masutti, F. Tomasello, *International Regulation of Non-Military Drones*, Cheltenham, 2018; E. Palmerini, M.A. Biasiotti, G.F. Aiello (a cura di), *Diritto dei droni. Regole, questioni e prassi*, Milano, 2018; M. Huttunen, *Safety and Security of Unmanned Aircraft Systems: Legislating Sociotechnical Change in Civil Aviation*, Rovaniemi, 2020; B.I. Scott, B. Custers, H. Lahmann, *Drone Regulation and AI Law: Assessing the Intersection of the EU Legal Frameworks for Unmanned Aircraft and Artificial Intelligence*, in *Air and Space Law*, 49 (2024), n. 6, p. 565 ss.

⁵ P.G. Chiara, *The Commission Action Plan on Drone and Counter Drone Security*, in *MediaLaws*, 25 marzo 2026, in <https://www.medialaws.eu/the-commission-action-plan-on-drone-and-counter-drone-security/>, che richiama F. Casolari, *Supranational Security and National Security in Light of the EU Strategic Autonomy Doctrine: The EU-Member States Security Nexus Revisited*, in *European Foreign Affairs Review*, 28 (2023), n. 4, p. 323 ss. L'autore osserva anche che il Piano non

Ciò non significa che ogni misura con finalità di sicurezza sia sottratta all'Unione: la disciplina aeronautica, dei prodotti e delle telecomunicazioni incide legittimamente su profili di *security*. I dubbi, ora di base giuridica ora di proporzionalità, riguardano tre misure in particolare:

- a) la registrazione con verifica dell'identità, perseguita con atti della Commissione fondati su un regolamento di sicurezza aerea (§ 3);
- b) il rilevamento tramite le reti mobili, che pone un problema di proporzionalità rispetto alla riservatezza delle comunicazioni (§ 5);
- c) il finanziamento tramite SAFE, adottato sulla base dell'art. 122 TFUE e impugnato dal Parlamento europeo (§ 7).

La scelta ha un costo: dove nessun titolo settoriale è disponibile, il Piano non va oltre la raccomandazione o l'invito. È ciò che accade per i poteri di neutralizzazione (§ 6), che pure il documento indica come la lacuna più grave dell'assetto attuale.

3. – L'intervento normativo più immediato è il *Drone Security Package*, annunciato dal Piano per il terzo trimestre 2026. Non si tratta di un nuovo regolamento, ma della modifica degli atti di esecuzione e delegati adottati sulla base del regolamento (UE) 2018/1139: il regolamento di esecuzione (UE) 2019/947 sulle operazioni e il regolamento delegato (UE) 2019/945 sui requisiti dei sistemi ⁶. Il Piano ne indica quattro contenuti: registrazione obbligatoria

chiarisce se sarà proposto un sistema di certificazione della cibersicurezza dei droni ai sensi del regolamento (UE) 2019/881 («regolamento sulla cibersicurezza»).

⁶ Regolamento (UE) 2018/1139 del Parlamento europeo e del Consiglio, del 4 luglio 2018, recante norme comuni nel settore dell'aviazione civile, che istituisce un'Agenzia dell'Unione europea per la sicurezza aerea e che modifica i regolamenti (CE) n. 2111/2005, (CE) n. 1008/2008, (UE) n. 996/2010, (UE) n. 376/2014 e le direttive 2014/30/UE e 2014/53/UE del Parlamento europeo e del Consiglio, e abroga i regolamenti (CE) n. 552/2004 e (CE) n. 216/2008 del Parlamento europeo e del Consiglio e il regolamento (CEE) n. 3922/91 del Consiglio, in GU UE L 212 del 22 agosto 2018; regolamento delegato (UE) 2019/945 della Commissione, del 12 marzo 2019, relativo ai sistemi aeromobili senza equipaggio e agli operatori di paesi terzi di sistemi aeromobili senza equipaggio, in GU UE L 152 dell'11 giugno 2019; regolamento di esecuzione (UE) 2019/947 della Commissione, del 24 maggio 2019, relativo a norme e procedure per l'esercizio di aeromobili senza equipaggio, in GU UE L 152 dell'11 giugno 2019. Sul quadro italiano dei mezzi aerei a pilotaggio remoto, v. ora M. Lamon, *I droni nel diritto della navigazione. Verso l'integrazione degli Unmanned Aircraft System nello spazio aereo non segregato*, Bari, 2025, spec. p. 52 ss. sul passaggio all'approccio *operation centric and risk based*; p. 62 s. sulla competenza nazionale in materia di pubblica sicurezza (art. 56, par. 8, reg. 2018/1139) e sulle zone geografiche UAS (art. 15 reg.

di tutti gli operatori di droni oltre i 100 g; estensione a tali droni dell'identificazione remota diretta; impossibilità di decollo senza l'inserimento del numero di registrazione dell'operatore; misure di semplificazione per alcune operazioni in vista e oltre la linea di vista, con il superamento dell'autorizzazione preventiva.

Il procedimento è stato rapido. L'EASA ha avviato una consultazione mirata (NPA 2026-103) e il 18 settembre 2026, poco più di sette mesi dopo il Piano, ha adottato il parere n. 06/2026, con i progetti dei due regolamenti di modifica ⁷. Il parere propone, per le operazioni nella categoria «aperta», di assogget-

2019/947); p. 116 ss. sul regolamento ENAC UAS-IT, sulla registrazione su D-Flight e sul codice QR; p. 139 ss. sulla responsabilità dell'operatore e sul *drone strike*; p. 159 ss. sulla protezione dei dati personali, e in particolare p. 168 s. sul considerando 31 e sull'allegato IX, punto 1.3, del reg. 2018/1139 e p. 170, ove si afferma che il requisito della registrazione «risponda ad esigenze di pubblica sicurezza (*security*) [...] piuttosto che a finalità di mera *safety*»; per una recensione, N. Romana, in questa *Rivista*, 2026, p. 797 ss. Della stessa Autrice, in questa *Rivista*, *Il ruolo dei mezzi aerei a pilotaggio remoto durante l'emergenza sanitaria del Covid-19*, 2020, p. 177 ss., con ampi riferimenti. Sulla responsabilità per danni a terzi in superficie, U. La Torre, *La navigazione degli UAV: un'occasione di riflessione sull'art. 965 c. nav. in tema di danni a terzi sulla superficie*, in *Riv. dir. nav.*, 2012, p. 553 ss.; sulle collisioni con aeromobili con equipaggio, M. Brignardello, *Collisioni tra mezzi aerei senza equipaggio e aeromobili tradizionali: misure di prevenzione e responsabilità in caso di drone strike*, in *Riv. dir. nav.*, 2018, p. 439 ss. V. inoltre E.G. Rosafio, *Considerazioni sui mezzi aerei a pilotaggio remoto e sul regolamento Enac*, in *Riv. dir. nav.*, 2014, p. 787 ss.; A.L.M. Sia, *Profili attuali della disciplina giuridica dei mezzi aerei a pilotaggio remoto ed il regolamento dell'Ente nazionale dell'aviazione civile italiana (ENAC)*, in *Dir. trasp.*, 2014, p. 743 ss.; B. Franchi, *Aeromobili senza pilota (UAV): inquadramento giuridico e profili di responsabilità*, in *Resp. civ. prev.*, 2010, parte I, p. 732 ss.; parte II, p. 1213 ss.; A. Masutti, *Prospettive di regolamentazione dell'uso dei velivoli senza pilota (UAV) nello spazio aereo comune*, in *Dir. trasp.*, 2007, p. 783 ss.; A. Zampone, *Riflessioni in tema di responsabilità nell'esercizio di Remotely-Piloted Aircraft System (RPAS)*, in *Dir. trasp.*, 2015, p. 63 ss.; C. Severoni, *La disciplina normativa attuale degli aeromobili a pilotaggio remoto*, in *Dir. trasp.*, 2016, p. 65 ss.; S. Panzeri, *I sistemi aerei a pilotaggio remoto (SAPR): profili giuridici*, in questa *Rivista*, 2016, p. 42 ss.; L. Mattioni, *Nuove prospettive per una regolamentazione europea dei sistemi aerei a pilotaggio remoto*, in *Riv. dir. nav.*, 2017, p. 719 ss.

⁷ EASA, NPA 2026-103, *Regular update of Regulations (EU) 2019/945 and (EU) 2019/947 — Simplification and security*; EASA, Opinion No 06/2026, *Regular update of Regulations (EU) 2019/947 and (EU) 2019/945 — Security*, 18 settembre 2026, in <https://www.easa.europa.eu/en/document-library/opinions/opinion-no-062026>, con i progetti di regolamento di esecuzione e delegato, che contengono anche le disposizioni transitorie richiamate nel testo. Il parere tratta esclusivamente le misure di sicurezza; le semplificazioni, oggetto della stessa NPA 2026-103, saranno proposte in un parere separato previsto per il quarto trimestre 2026. Sullo stato del procedimento dopo il parere, *Dronezine*, 19 settembre 2026, in <https://www.dronezine.it/?p=460021>, secondo cui le modifiche «diventeranno effettive solo dopo l'eventuale adozione da parte della Commissione europea».

tare alla registrazione gli operatori di UAS con massa al decollo pari o superiore a 100 g e di estendere a tali aeromobili l'obbligo di identificazione remota diretta, salve le deroghe e le disposizioni transitorie previste dai progetti. Aggiunge inoltre un elemento che il Piano non menzionava: l'obbligo per gli Stati membri di verificare l'identità dell'operatore prima della registrazione. Interviene poi sulle zone geografiche UAS, introducendo «condizioni nazionali» per rendere più accessibili e uniformi le informazioni sulle operazioni, ma conserva il carattere discrezionale del potere degli Stati di istituirle: richiede che le misure siano necessarie e proporzionate al rischio quando perseguono finalità di *safety*, di tutela della riservatezza e dei dati personali o di protezione dell'ambiente. Le misure adottate per ragioni di *security* restano fuori da questa specifica previsione, senza che ciò le sottragga ai limiti generali richiamati in premessa. Prevede inoltre che l'identificazione remota diretta possa non essere imposta agli aeromodelli operati nell'ambito di club e associazioni. Alla data di questo commento la Commissione non risulta aver ancora adottato gli atti, che il Piano annunciava per il terzo trimestre 2026. Il parere prevede inoltre tempi di adeguamento lunghi: le nuove regole sulle zone geografiche si applicherebbero dodici mesi dopo l'entrata in vigore; per i droni già immessi sul mercato non sarebbe richiesta a posteriori la funzione di blocco al decollo, quelli fino a 900 g sarebbero esentati dall'installare un dispositivo aggiuntivo di identificazione remota diretta e quelli più pesanti avrebbero quarantotto mesi dall'entrata in vigore per farlo ⁸.

Tre osservazioni.

a) *La base giuridica*. Il quadro del 2019 nasce come disciplina di *safety*, costruita sulla proporzionalità al rischio operativo. Il regolamento 2018/1139 contiene però già il germe della *security*: il considerando 31 fonda l'immatricolazione degli aeromobili senza equipaggio e dei loro operatori sui rischi per la sicurezza, la riservatezza, i dati personali, la *security* e l'ambiente, e l'allegato IX, punto 1.3, impone le caratteristiche e funzionalità necessarie ad attenuarli. Già nel quadro del 2019, del resto, si è osservato che la registrazione degli operatori risponde a esigenze di pubblica sicurezza più che di mera *safety* ⁹. La no-

⁸ V. *supra*, nota 7.

⁹ V. *supra*, nota 6. Valorizza invece la funzione di protezione dei dati personali della registrazione, quale «crucial interface» tra disciplina aeronautica e regolamento 2016/679, E. Vermiglio, *UAS and Data Protection*, in M.P. Rizzo, F. Franchina (a cura di), *Drones in the Digital European Sky. Theoretical Foundations and Aviation Law Perspectives*, Cham, 2025, p. 207 ss., spec. p. 213 ss., che riconduce la protezione dei dati a un interesse pubblico idoneo a orientare la discrezionalità degli

vità del 2026 non è quindi la comparsa della *security*, ma il suo passaggio da finalità concorrente a finalità prevalente. La prevalenza non si desume soltanto dal linguaggio del Piano, ma dalla struttura dell'intervento. Il Piano accompagna le misure di sicurezza con semplificazioni commisurate al rischio operativo, come il superamento dell'autorizzazione preventiva per alcune operazioni in vista e oltre la linea di vista; l'EASA le ha però scorporate dal parere n. 06/2026, che tratta soltanto la sicurezza, e le annuncia in un parere distinto per il quarto trimestre 2026. Il parere contiene solo attenuazioni puntuali, come quella riguardante i club e le associazioni di aeromodellismo, per i quali l'identificazione remota diretta può essere esclusa nell'autorizzazione rilasciata dall'autorità competente. I nuovi obblighi (registrazione e identificazione remota a partire da 100 g, verifica dell'identità e blocco al decollo) opererebbero invece, nei rispettivi ambiti di applicazione e salve le deroghe previste, a prescindere dal rischio della singola operazione e servirebbero a rendere identificabili il mezzo e chi lo opera. L'alleggerimento della *safety* dove il rischio è basso è per ora soltanto annunciato, mentre la *security* verrebbe estesa anche dove il rischio è basso. Ed è proprio l'apertura del regolamento base alla *security* che permette di perseguire obiettivi di sicurezza pubblica con atti della Commissione, senza un nuovo intervento del legislatore. Il risultato è efficace ma non privo di ambiguità: misure che incidono sulla libertà di un numero molto ampio di utenti ricreativi sono adottate attraverso atti di esecuzione e delegati, con un controllo parlamentare più debole, e diverso a seconda del tipo di atto. Sugli atti delegati il Parlamento europeo e il Consiglio possono sollevare obiezioni che ne impediscono l'entrata in vigore (art. 290, par. 2, TFUE). Gli atti di esecuzione sono invece adottati sotto il controllo degli Stati membri riuniti in comitato: il Parlamento e il Consiglio possono soltanto segnalare alla Commissione che il progetto eccede le competenze di esecuzione, e la Commissione è tenuta a riesaminarlo ma non a modificarlo (art. 11 reg. (UE) n.

Stati alla stregua dell'ordine pubblico e della sicurezza nazionale (art. 56, par. 8, reg. 2018/1139; art. 15 reg. 2019/947). Il contributo è pubblicato anche in versione italiana: E. Vermiglio, *Droni e tutela dei dati personali*, in questa *Rivista*, 2025, suppl. *ATM, Drones and Digitalization, Artificial Intelligence and New Technologies for Environment*, p. 419 ss., spec. p. 430 ss. Sull'interdipendenza tra *safety* e *security* negli artt. 4 e 88 del reg. 2018/1139 e sulla nozione di *security* ricavata dall'Annesso 17 alla Convenzione di Chicago, come tutela contro gli atti di interferenza illecita, A. Masutti, F. Tomasello, *Security Issues*, in B.I. Scott (a cura di), *The Law of Unmanned Aircraft Systems*, cit., p. 144 s. (v. anche *infra*, nota 26).

182/2011). In nessuno dei due casi il testo è emendabile. Il problema non riguarda dunque l'esistenza della competenza, ma il suo limite. Le norme essenziali di una materia sono riservate al legislatore dell'Unione (art. 290, par. 1, TFUE), e vi rientrano, secondo la Corte di giustizia, le disposizioni la cui adozione richiede scelte politiche e una ponderazione di interessi divergenti, e in particolare quelle che consentono ingerenze incisive nei diritti fondamentali¹⁰. La verifica dell'identità degli operatori, che il Piano non menzionava e che l'EASA ha aggiunto, ha i tratti di una scelta di questo tipo. Si può obiettare che la verifica non introduca un obbligo nuovo, ma definisca soltanto le modalità per rendere attendibile una registrazione già prevista dal regolamento di base e dagli atti del 2019, e che non abbia nulla dei poteri coercitivi esaminati dalla Corte. L'obiezione coglie un dato reale, ma non è decisiva. Il criterio della Corte non guarda alla sola coercizione, ma all'intensità dell'ingerenza e alla natura politica della scelta. E la verifica dell'identità non si limita a perfezionare la registrazione: ne accentua la funzione di filtro di pubblica sicurezza, affiancandola a quella di responsabilizzazione dell'operatore, e comporta un trattamento di dati personali su larga scala riferito a un'ampia platea di utenti ricreativi. È questa combinazione, più che il singolo adempimento, a suggerire che la scelta spetti al legislatore.

b) *La funzione della registrazione.* Sarebbe ingenuo attendersi che l'operatore malintenzionato adempia agli obblighi di registrazione e renda identificabile il mezzo. La funzione della nuova disciplina è un'altra: rendere identificabile in tempo reale la quasi totalità dei droni legittimi, così che i droni che, pur essendovi soggetti, non trasmettono una valida identificazione possano essere trattati come non cooperativi. È un indicatore operativo, non una qualificazione giuridica: la mancata identificazione segnala un'anomalia da verificare, ma non dimostra da sola un'intenzione ostile. La registrazione diventa in questo senso un presupposto non del rilevamento, che il § 5 mostra possibile anche per oggetti non connessi, ma dell'identificazione e della qualificazione dei mezzi rilevati: è il filtro che permette alle autorità di distinguere, come dice il Piano, gli

¹⁰ Corte giust., 5 settembre 2012, causa C-355/10, *Parlamento c. Consiglio*, punti 64-67 e 76-78, che ha annullato la decisione 2010/252/UE sulla sorveglianza delle frontiere marittime esterne, adottata con procedura di comitato: per la Corte il carattere essenziale va accertato su elementi oggettivi, sottoposti a sindacato giurisdizionale (punto 67), e l'attribuzione di poteri di pubblico imperio comporta ingerenze nei diritti fondamentali «talmente incisive [...] da rendere necessario l'intervento del legislatore dell'Unione» (punto 77).

amici dai nemici. La riduzione della soglia da 250 a 100 g, già adottata dal Regno Unito dal 1° gennaio 2026¹¹, risponde alla stessa logica: amplia la fascia di operatori soggetti a obblighi uniformi, comprendendo i diffusissimi modelli tra 100 e 250 g dotati di fotocamera, per i quali oggi l'obbligo di registrazione dipende dalla presenza di sensori in grado di raccogliere dati personali e l'identificazione remota diretta non è richiesta.

c) *Il prodotto e l'operatore*. Il divieto di decollo senza numero di registrazione è un requisito di progettazione che grava sul fabbricante e trova la sua sede nel regolamento delegato 2019/945. Il regime transitorio evita di imporre retroattivamente questa funzione ai droni già immessi sul mercato; resta distinto il problema dell'adeguamento all'identificazione remota diretta, per il quale sono previste esenzioni e scadenze differenziate. Quanto al blocco al decollo, il limite è soprattutto quello di un formalismo agevolmente eludibile se il numero inserito non è verificato da remoto. La verifica dell'identità prima della registrazione proposta dall'EASA va nella direzione di rendere il dato affidabile, ma il trattamento di dati personali che comporta (v. *supra*, lett. a) dovrà essere giustificato alla luce del regolamento (UE) 2016/679 e delle regole di accesso ai dati poste dall'art. 74 del regolamento 2018/1139.

Il Piano prevede infine di migliorare entro il quarto trimestre 2026, ormai in corso, la pubblicazione digitale delle zone geografiche UAS e di definire entro il 2027 i requisiti tecnici del *geofencing*, oltre a sostenere una più rapida attuazione dei servizi U-space, ancora disomogenea tra gli Stati¹². In Italia la

¹¹ UK Civil Aviation Authority, Remote ID, requisiti in vigore dal 1° gennaio 2026, in <https://www.caa.co.uk/drones/drone-regulations/policy-programmes/remote-id-rid/>. Sul limite strutturale di registrazione e identificazione, che presuppongono la collaborazione dell'operatore e perciò scoraggiano poco chi intende agire illecitamente, M. Huttunen, *Civil Unmanned Aircraft Systems and Security: The European Approach*, in *Journal of Transportation Security*, 12 (2019), p. 83 ss.

¹² Regolamento di esecuzione (UE) 2021/664 della Commissione, del 22 aprile 2021, su un quadro normativo per lo U-space; regolamento di esecuzione (UE) 2021/665 della Commissione, del 22 aprile 2021, che modifica il regolamento di esecuzione (UE) 2017/373 per quanto riguarda i requisiti per i fornitori di servizi di gestione del traffico aereo/servizi di navigazione aerea e di altre funzioni della rete di gestione del traffico aereo nello spazio aereo U-space designato nello spazio aereo controllato; regolamento di esecuzione (UE) 2021/666 della Commissione, del 22 aprile 2021, che modifica il regolamento (UE) n. 923/2012 per quanto riguarda i requisiti per l'aviazione con equipaggio operante nello spazio aereo U-space; tutti in GU UE L 139 del 23 aprile 2021. ENAC, Regolamento UAS-IT, edizione 1 del 4 gennaio 2021, e circolare ATM-09A del 24 marzo 2021, elencati come vigenti nella pagina ENAC sulla normativa droni (aggiornata all'11 marzo 2026), in <https://www.enac.gov.it/normativa-droni>; la bozza del 2024 di una nuova edizione di UAS-IT non

pubblicazione delle zone geografiche passa ancora per il regolamento ENAC UAS-IT, nella prima edizione del 4 gennaio 2021, per la circolare ATM-09A e per il servizio D-Flight. Nel giugno 2026 l'ENAC ha diffuso la bozza di un regolamento dedicato alle zone geografiche UAS, che prevede la possibilità di istituire zone vietate per motivi di sicurezza o di ordine pubblico su richiesta delle prefetture, delle istituzioni militari o di altre amministrazioni dello Stato. L'esperienza nazionale potrà essere utile nella definizione delle condizioni comuni ¹³.

4. – La seconda linea di prevenzione riguarda la resilienza dei beni da proteggere. Il riferimento è la direttiva (UE) 2022/2557 sulla resilienza dei soggetti critici, attuata in Italia con il d.lgs. 4 settembre 2024, n. 134 ¹⁴. Il Piano ne

risulta adottata. ENAC, bozza di Regolamento Zone geografiche UAS, giugno 2026, art. 4, par. 2, in https://www.enac.gov.it/app/uploads/2026/06/2026_06_22-Bozza-Reg-Zone-geografiche-UAS.pdf. Sullo U-space, M. Lamon, *I droni nel diritto della navigazione*, cit., p. 207 ss., e p. 210 s. sui servizi di base (registrazione, identificazione elettronica e geo-consapevolezza) già disciplinati dal reg. 2019/947 (considerando 26, artt. 14 e 15); sul *geofencing* come forma di regolazione *by design*, ivi, p. 2, nt. 6, e p. 169, ove si richiama l'art. 28 del regolamento UAS-IT sulla responsabilità dell'operatore di verificare le restrizioni disposte dall'Autorità di pubblica sicurezza. Sullo U-space e sulla mobilità aerea innovativa v. inoltre, in questa *Rivista*, 2025, suppl. *ATM, Drones and Digitalization, Artificial Intelligence and New Technologies for Environment*: M.P. Rizzo, *I servizi U-Space: dalla certificazione del fornitore all'accesso alla fornitura. Profili qualificatori e disciplinari*, p. 257 ss.; L. Brucculeri, *Deployment in Italia delle soluzioni U-Space (CISP e USSP). D-Flight prima società certificata*, p. 277 ss.; C. Ingratoci, *Mobilità aerea innovativa e trasporto urbano: la Urban Air Mobility e sue prospettive di implementazione*, p. 285 ss.; G. Ferrara, *ATM & U-Space Services to support the Urban Air Mobility Airspace Integration Challenges*, p. 315 ss.; A. Marino, *Droni, mobilità urbana e infrastrutture. I vertiporti*, p. 347 ss. Sul quadro nazionale e sovranazionale delle operazioni, M. Pandolfino, *Le operazioni degli aeromobili a pilotaggio remoto nella normativa nazionale e sovranazionale*, ivi, p. 185 ss.

¹³ V. *supra*, nota 12.

¹⁴ Direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa alla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE del Consiglio, in GU UE L 333 del 27 dicembre 2022; d.lgs. 4 settembre 2024, n. 134 (GU n. 223 del 23 settembre 2024). La Strategia nazionale per la resilienza dei soggetti critici prevista dall'art. 6 del decreto è stata adottata dal Presidente del Consiglio dei ministri nell'aprile 2026 e pubblicata l'11 giugno 2026; il termine per l'adozione era fissato al 17 luglio 2025 dall'art. 6, comma 1, del decreto, in anticipo rispetto a quello del 17 gennaio 2026 previsto dall'art. 4, par. 1, della direttiva. Gli orientamenti della Commissione seguono un approccio multirischio; il Piano (§ 2.2.2) ne preannunciava indicazioni specifiche sui droni e sul geofencing: Commissione europea, Orientamenti sull'applicazione dell'articolo 13, paragrafo 5, della direttiva (UE) 2022/2557 sulla resilienza dei soggetti critici, C/2026/3712, in GU UE C del 13 luglio 2026, in <https://eur-lex.europa.eu/legal-content/IT/>

chiede l'attuazione «urgente e completa» e annuncia per il secondo trimestre 2026 orientamenti non vincolanti sulle misure di resilienza, con indicazioni specifiche sui droni e sul *geofencing* (la Commissione li ha poi pubblicati il 13 luglio 2026); prevede inoltre un piano volontario di *stress test* delle infrastrutture critiche contro le intrusioni di droni, sul modello di quelli già condotti per l'energia e i cavi sottomarini. In Italia gli orientamenti europei sono giunti in una fase di prima attuazione: la Strategia nazionale prevista dal decreto è stata adottata solo nell'aprile 2026 e pubblicata l'11 giugno, con un ritardo di circa nove mesi alla data di adozione, e di quasi undici alla pubblicazione, sul termine del 17 luglio 2025 fissato dal decreto.

Per il diritto dei trasporti il dato più rilevante è un'assenza. Aeroporti e porti compaiono più volte tra i beni esposti, ma il Piano non richiama mai il regolamento (CE) n. 300/2008 sulla *security* dell'aviazione civile, né il regolamento (CE) n. 725/2004 e la direttiva 2005/65/CE sulla sicurezza delle navi e dei porti ¹⁵. Sono discipline che già organizzano, con programmi nazionali, valutazioni

TXT/PDF/?uri=OJ:C_202603712.

¹⁵ Regolamento (CE) n. 300/2008 del Parlamento europeo e del Consiglio, dell'11 marzo 2008, che istituisce norme comuni per la sicurezza dell'aviazione civile e che abroga il regolamento (CE) n. 2320/2002, in GU UE L 97 del 9 aprile 2008; regolamento di esecuzione (UE) 2015/1998 della Commissione, del 5 novembre 2015, che stabilisce disposizioni particolareggiate per l'attuazione delle norme fondamentali comuni sulla sicurezza dell'aviazione civile, in GU UE L 299 del 14 novembre 2015; regolamento (CE) n. 725/2004 del Parlamento europeo e del Consiglio, del 31 marzo 2004, relativo al miglioramento della sicurezza delle navi e degli impianti portuali, in GU UE L 129 del 29 aprile 2004; direttiva 2005/65/CE del Parlamento europeo e del Consiglio, del 26 ottobre 2005, relativa al miglioramento della sicurezza dei porti, in GU UE L 310 del 25 novembre 2005. Già prima del Piano si era sostenuto che la competenza dell'Unione in materia di *security* aeroportuale, esercitata con il regolamento n. 300/2008, consentirebbe di imporre sistemi antidrone almeno negli scali di maggior traffico: M. Huttunen, *Civil Unmanned Aircraft Systems and Security*, cit., p. 97 s. Nel senso che il gestore aeroportuale, quale responsabile della *safety* e della *security* del sedime (allegato VII, punto 2.1, reg. 2018/1139), potrebbe dotarsi di sistemi counter-UAS, M. Lamon, *I droni nel diritto della navigazione*, cit., p. 158, che rinvia a E. Sabatino, *Contrasto delle nuove minacce*, in E. Sabatino, F. Pettinari (a cura di), *La minaccia dei droni duali e le sfide per l'Italia*, Roma, 2020 (Documenti IAI, 20|04), p. 51 ss. Il vigente Annesso 17 alla Convenzione di Chicago (12^a ed., emendamento 18, applicabile dal 18 novembre 2022) non menziona gli aeromobili senza equipaggio, ma impone agli Stati di tenere costantemente sotto esame il livello e la natura della minaccia nel proprio territorio e nello spazio aereo sovrastante, adeguando il programma nazionale di sicurezza sulla base di una valutazione del rischio (norma 3.1.3), e di adottare misure contro gli attacchi agli aeromobili in aeroporto o nelle sue vicinanze condotti con MANPADS «and other weapons representing a similar threat» (norma 4.3.6): formule abbastanza ampie da

del rischio e piani di sicurezza, la protezione di questi stessi luoghi contro atti illeciti intenzionali. E non mancano strumenti già dedicati ai droni: gli orientamenti dell'EASA sulla gestione degli eventi drone negli aeroporti riconducono il drone non autorizzato ai pericoli che il gestore deve governare con il proprio sistema di gestione della sicurezza, in collaborazione con i servizi del traffico aereo e con le forze di polizia, e danno conto di programmi nazionali per la sicurezza dell'aviazione civile che contengono già disposizioni specifiche. L'unico raccordo esplicito del Piano con il settore è il richiamo al codice frontiere Schengen, che secondo il Piano consente misure antidrone civili a protezione delle frontiere e, per estensione, dei perimetri di sicurezza aeroportuali¹⁶. Il Piano non indica però la disposizione su cui fonda l'affermazione, e l'art. 13, sulla sorveglianza di frontiera, consente l'uso di «mezzi tecnici, compresi i mezzi elettronici», ma non menziona i droni né le misure antidrone: la lettura della Commissione è dunque estensiva, tanto più quando la riferisce ai perimetri aeroportuali. Il silenzio del Piano non significa che nell'ordinamento manchi un raccordo, ma lascia aperta la questione di come gli obblighi di resilienza si coordinino con quelli settoriali di *security*. La direttiva CER contiene un criterio di coordinamento: le sue pertinenti disposizioni non si applicano quando atti settoriali dell'Unione impongono misure di resilienza che gli Stati riconoscono almeno equivalenti ai corrispondenti obblighi (art. 1, par. 3). Resta però da verificare in quale misura gli obblighi settoriali di *security* aeroportuale e portuale coprano anche la minaccia dei droni, e possano quindi dirsi equivalenti sotto questo profilo. In caso contrario,

comprendere i droni, che l'ICAO tratta in un documento di orientamento dedicato, *Protection of Civil Aviation Infrastructure Against Unmanned Aircraft*, in <https://www.icao.int/aviation-security-policy-section/uas-intrusion-protection>. Sugli eventi drone negli aeroporti, EASA, *Drone Incident Management at Aerodromes*, Part 1, *The challenge of unauthorised drones in the surroundings of aerodromes*, Part 2, *Guidance and recommendations*, Part 3, *Resources and practical tools*, Colonia, 2021, in https://www.easa.europa.eu/sites/default/files/dfu/drone_incident_management_at_aerodromes_part1_website_suitable.pdf.

¹⁶ Regolamento (UE) 2016/399 del Parlamento europeo e del Consiglio, del 9 marzo 2016, che istituisce un codice unionale relativo al regime di attraversamento delle frontiere da parte delle persone (codice frontiere Schengen), in GU UE L 77 del 23 marzo 2016, come modificato dal regolamento (UE) 2024/1717 del Parlamento europeo e del Consiglio, del 13 giugno 2024, in GU UE L del 20 giugno 2024. Sul sistema europeo di sorveglianza delle frontiere (EUROSUR), regolamento (UE) 2019/1896 del Parlamento europeo e del Consiglio, del 13 novembre 2019, relativo alla guardia di frontiera e costiera europea e che abroga i regolamenti (UE) n. 1052/2013 e (UE) 2016/1624, in GU UE L 295 del 14 novembre 2019.

lo stesso gestore aeroportuale o portuale potrebbe trovarsi destinatario di obblighi di resilienza come soggetto critico, di misure di *security* come gestore di uno scalo e, domani, di eventuali obblighi antidrone, con valutazioni del rischio, piani e autorità di vigilanza diversi. Un'integrazione della minaccia dei droni nei programmi di *security* aeroportuale e portuale sarebbe la via più lineare.

Gli spazi marittimi ricevono un'attenzione specifica, perché porti, impianti energetici in mare e cavi sottomarini sono esposti a droni aerei, di superficie e subacquei. La risposta proposta è la *consapevolezza situazionale marittima* (*maritime domain awareness*), cioè la capacità di sapere in tempo quasi reale che cosa si muove in un tratto di mare, incrociando i dati di radar, satelliti, sistemi di identificazione delle navi e sensori subacquei. Il Piano prevede entro il 2027 un'azione pilota in questa direzione.

L'azione non crea una struttura nuova, ma si innesta sui *Regional Cable Hubs*. Si tratta dei centri regionali previsti dal Piano d'azione sulla sicurezza dei cavi del febbraio 2025, che mettono in comune tra gli Stati rivieraschi informazioni e capacità di rilevamento delle anomalie attorno ai cavi sottomarini. I primi due, finanziati nel giugno 2026, riguardano il Baltico e il Mediterraneo; quest'ultimo è coordinato dall'Italia. Il Piano ne propone un doppio ampliamento: dai cavi a tutte le infrastrutture marittime critiche, e dalla sorveglianza tradizionale all'impiego di droni e al monitoraggio delle minacce che i droni stessi rappresentano.

All'azione partecipano le tre agenzie dell'Unione che esercitano funzioni di guardia costiera: l'EMSA per la sicurezza marittima e la sorveglianza del traffico navale, l'EFCA per il controllo della pesca e Frontex per le frontiere. È previsto anche il collegamento con MARSUR, la rete con cui l'Agenzia europea per la difesa mette in comunicazione i sistemi di sorveglianza delle marine militari, e con i sistemi della NATO. È uno dei punti in cui la cooperazione civile-militare, tratto caratteristico del Piano (§ 7), diventa più stretta ¹⁷.

¹⁷ Comunicazione congiunta, *Piano d'azione dell'UE sulla sicurezza dei cavi*, JOIN(2025) 9 final, 21 febbraio 2025. Sui primi due Regional Cable Hubs, Commissione europea, comunicato stampa IP/26/1429, *Commission funds first Regional Cable Hubs and launches €40 million call for cable repair capacity*, 23 giugno 2026, in https://ec.europa.eu/commission/presscorner/detail/en/ip_26_1429: l'hub del Baltico (2,5 milioni di euro) è coordinato dalla Finlandia con Danimarca, Germania, Estonia, Lettonia e Svezia; quello del Mediterraneo (3,3 milioni) dall'Italia; i progetti sono finanziati dalla Commissione. Lo stesso comunicato annuncia un bando CEF Digitale da 40 milioni per moduli di riparazione dei cavi nel Mediterraneo e nell'Atlantico e un nuovo ban-

L'estensione ai droni di superficie e subacquei è significativa, perché questi mezzi restano estranei al quadro aeronautico e la loro disciplina, sul piano internazionale, si intreccia con il codice internazionale per le navi autonome di superficie (MASS Code), adottato dal Comitato per la sicurezza marittima dell'IMO nel maggio 2026 come strumento non vincolante, applicabile dal 1° luglio 2026, in vista di una versione obbligatoria da adottare entro il 2030¹⁸. L'intreccio è però parziale: il codice riguarda le navi da carico soggette alla convenzione SOLAS, in genere di stazza superiore a 500 GT in viaggi internazionali, ed è destinato, secondo la roadmap dell'IMO, a diventare obbligatorio mediante emendamenti alla stessa convenzione; ne restano fuori i droni subac-

do, nell'autunno 2026, per estendere gli hub ad altri bacini o ad altri Stati membri. Sul punto, Piano, § 2.2.2. Sulla tutela dei cavi sottomarini e sulla legge n. 9 del 2026, G. Gugliotti, *La tutela dei cavi sottomarini: l'Italia aggiorna la difesa delle reti subacquee*, in questa *Rivista*, 2026, p. 161 ss., spec. p. 169 s. sull'Agenzia e p. 162 sui droni subacquei come tecnologia dual use; v. anche C. Vagaggini, *Il regime giuridico dei cavi sottomarini: gli sviluppi normativi nello scenario internazionale, europeo e nazionale*, in *Riv. dir. nav.*, 2022, n. 1, p. 179 ss.; F. Martini, *La protezione dei cavi sottomarini fra intervento pubblico e interesse alla libertà dei mari*, in *Mercato Concorrenza Regole*, 2024, n. 1-2, p. 275 ss. Legge 26 gennaio 2026, n. 9, in GU n. 21 del 27 gennaio 2026, spec. artt. 4, 6, 13 e 30; gli artt. 10 e, in parte, 16 si applicano dal 1° gennaio 2027.

¹⁸ IMO, Maritime Safety Committee, 111^a sessione, 13-22 maggio 2026, che ha adottato l'*International Code of Safety for Maritime Autonomous Surface Ships* (MASS Code) come strumento non obbligatorio, con effetto dal 1° luglio 2026, avviando una fase di acquisizione dell'esperienza in vista di un codice obbligatorio; il codice riconduce i centri di controllo remoto al regime di *security* del codice ISPS, attraverso la valutazione e il piano di sicurezza della nave: Indian Register of Shipping, *IMO Maritime Safety Committee (MSC), 111th Session, 13-22 May 2026. Session Outcome*, p. 4 s., in <https://www.irclass.org/media/8535/msc-111-report.pdf>. Il codice si applica alle navi da carico soggette al capitolo I della convenzione SOLAS, ma se ne raccomanda l'applicazione, per quanto possibile, anche alle unità di stazza inferiore a 500 GT; secondo la roadmap dell'IMO, l'elaborazione del codice obbligatorio, da avviare nel 2028, comprenderà l'esame di emendamenti alla SOLAS (nuovo capitolo), con adozione prevista entro il 1° luglio 2030 ed entrata in vigore il 1° gennaio 2032: IMO, *FAQ – Autonomous shipping*, in <https://www.imo.org/en/mediacentre/hottopics/pages/autonomous-shipping.aspx>. In dottrina, M. Menicucci, *Le Unmanned Ships: profili applicativi e problemi normativi. La nave, l'equipaggio, il comandante, il diporto*, Bari, 2023, spec. p. 43 ss. sul codice, allora annunciato come strumento non vincolante, p. 104 ss. sulla nozione di nave nel diritto internazionale, p. 172 ss. sul rapporto tra centro di controllo remoto ed equipaggio e p. 187 ss. su quello tra comandante e centro di controllo a terra. Nel diritto italiano, l'unità da diporto a comando remoto, definita come unità «priva a bordo di personale adibito al comando» (art. 3, comma 1, lett. h-bis, d.lgs. 18 luglio 2005, n. 171), è comandata da chi ne esercita il controllo remoto, che ne «assume e mantiene il comando» (art. 27-bis, comma 3), ma può imbarcare incaricati del proprietario o dell'armatore che intervengano in caso di pericolo o di necessità (art. 27-bis, comma 2): *ivi*, p. 255 ss.

quei e gran parte dei droni di superficie di piccole dimensioni, ai quali gli Stati sono soltanto invitati ad applicarlo, per quanto possibile.

L'Italia si è mossa per tempo su questo terreno. La legge 26 gennaio 2026, n. 9, sulla sicurezza delle attività subacquee, istituisce l'Agenzia per la sicurezza delle attività subacquee, che autorizza la navigazione subacquea e il transito di mezzi stranieri e definisce le misure di protezione delle infrastrutture sottomarine soggette alla giurisdizione nazionale, compresi i cavi. La legge estende inoltre il codice della navigazione ai mezzi subacquei non militari, «con equipaggio, autonomi o a controllo remoto», e ne disciplina i requisiti di sicurezza e la qualificazione di chi li conduce. È una scelta che ricorda quella compiuta per i droni aerei con l'art. 743, comma 2, c. nav.: anche nell'ambiente subacqueo il mezzo senza equipaggio entra nel diritto della navigazione, e la sua disciplina nasce insieme dalla *safety* e dalla *security*. Il raccordo con l'azione pilota europea, e in particolare con l'hub mediterraneo, sarà un banco di prova ¹⁹.

Sul versante del mercato, il Piano combina tre strumenti. Il regolamento (UE) 2024/2847 sulla ciberresilienza, applicabile in via generale dall'11 dicembre 2027 ma con gli obblighi dei fabbricanti di segnalare le vulnerabilità attivamente sfruttate già applicabili dall'11 settembre 2026, assoggetterà a requisiti di sicurezza informatica la gran parte dei droni immessi sul mercato ²⁰.

¹⁹ V. *supra*, nota 17.

²⁰ Regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, relativo a requisiti orizzontali di cibersecurity per i prodotti con elementi digitali e che modifica i regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e la direttiva (UE) 2020/1828 (regolamento sulla ciberresilienza), in GU UE L del 20 novembre 2024. Il regolamento non si applica ai prodotti con elementi digitali certificati a norma del regolamento (UE) 2018/1139 (art. 2, par. 3). L'esclusione riguarda i droni della categoria certificata, la cui progettazione e produzione sono certificate secondo l'art. 40 del regolamento delegato (UE) 2019/945 e i regolamenti (UE) n. 748/2012 e 2015/640 (v. anche l'art. 3, lett. c), del regolamento di esecuzione 2019/947). Non riguarda invece i droni con marcatura di classe, immessi sul mercato con la marcatura CE all'esito delle procedure di valutazione della conformità previste dal regolamento 2019/945, anche con l'intervento di organismi notificati, e soggetti alla vigilanza del mercato del regolamento (UE) 2019/1020: S. Vernizzi, *La nozione di drone alla luce del panorama normativo vigente e delle future prospettive di sviluppo*, in questa Rivista, 2025, suppl. ATM, *Drones and Digitalization, Artificial Intelligence and New Technologies for Environment*, p. 153 ss., spec. p. 170; R. Avagliano, *Immissione sul mercato UAS, marcatura CE e definizione C-class*, ivi, p. 177 ss., spec. p. 177 e p. 181 s. Già dal 1° agosto 2025, inoltre, il regolamento delegato (UE) 2022/30 della Commissione, del 29 ottobre 2021, che integra la direttiva 2014/53/UE per quanto riguarda l'applicazione dei requisiti essenziali di cui all'art. 3, par. 3,

Un *EU Trusted Drone Label*, da definire entro il quarto trimestre 2026 e del quale alla metà di ottobre non sono ancora noti i contenuti, dovrebbe aggiungere criteri di affidabilità verificati da terzi, senza duplicare la legislazione esistente. Una valutazione coordinata dei rischi della catena di approvvigionamento ICT dei droni e dei sistemi antidrone, che il Piano prevedeva entro il terzo trimestre 2026 e che la Commissione ha già avviato con gli Stati membri, potrebbe condurre a un *toolbox* di misure di mitigazione. La pagina della Commissione dedicata al Piano parla apertamente di evitare i fornitori ad alto rischio: senza nominarli, il riferimento evoca il precedente del *toolbox* per la sicurezza del 5G e investe un mercato dei droni civili oggi largamente dipendente da produttori extraeuropei²¹. È il punto in cui la *security* si salda alla politica industriale, ed è anche quello in cui più forte è il rischio di misure che, pur legittime, operino come barriere commerciali.

Completa il quadro la minaccia dei palloni meteorologici lanciati da Paesi terzi a fini di contrabbando, per la quale il Piano prevede un gruppo di lavoro con gli Stati interessati e una sfida di innovazione rivolta alle imprese.

5. – La seconda parte del Piano muove da una constatazione: manca oggi una sorveglianza integrata dello spazio aereo per i droni, e i flussi informativi che servirebbero a costruirla non sono collegati tra loro. Le azioni sono quattro: integrare i dati in sistemi di visualizzazione unica, sul modello dello strumento CIMACTION sviluppato da Eurocontrol per il coordinamento civile-militare; rendere i dati accessibili alle autorità competenti, sulla base dell'art. 74 del regolamento 2018/1139; esplorare una piattaforma europea degli incidenti con droni, alimentata dalle segnalazioni obbligatorie e accessibile alle autorità nazionali; integrare il rilevamento nei sistemi nazionali di sorveglianza delle

lett. d), e) ed f), in GU UE L 7 del 12 gennaio 2022, applicabile da tale data per effetto del regolamento delegato (UE) 2023/2444 della Commissione, del 20 luglio 2023, impone requisiti di cybersecurity alle apparecchiature radio in grado di comunicare via internet, categoria in cui rientra gran parte dei droni connessi.

²¹ Commissione europea, Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures, in <https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures>, richiamato dal Piano (nota 21). Sull'avvio della valutazione coordinata dei rischi della catena di approvvigionamento ICT dei droni e dei sistemi antidrone, in vista di un possibile Drone and Counter-Drone Security Toolbox, Commissione europea, seguito dato alla risoluzione del Parlamento europeo del 22 gennaio 2026 (2025/2088(INI)), in https://data.europa.eu/parl.europa.eu/distribution/doc/SP-2026-05-26-TA-10-2026-0270_en.pdf.

frontiere e in EUROSUR (v. *supra*, nota 16). Gli Stati sono invitati a stabilire accordi pratici di condivisione delle informazioni tra aviazione civile, forze di polizia e forze armate.

L'elemento più innovativo, e giuridicamente più delicato, è l'uso delle reti mobili. Il Piano delinea un rilevamento a due livelli. Il primo sfrutta la capacità esistente delle reti per individuare i droni connessi attraverso anomalie nelle identità delle SIM, nei tipi di traffico e negli spostamenti, con sistemi di allerta basati sull'intelligenza artificiale. A questo si collega il concetto di «spazio aereo digitale»: la Commissione lavora a una decisione di esecuzione per armonizzare lo spettro utilizzabile dai droni nelle bande mobili e per subordinare la connessione alla rete a una pre-identificazione del terminale come drone. Il secondo livello, la *Integrated Sensing and Communication* (ISAC), trasforma le antenne 5G e di nuova generazione in sensori radar capaci di rilevare oggetti non connessi, palloni compresi. Per renderlo possibile occorre modificare le regole di attribuzione dello spettro: il Piano rinvia alla proposta di *Digital Networks Act* e annuncia un mandato alla CEPT, poi conferito dalla Commissione per la banda 3,4-3,8 GHz, in vista di una modifica della relativa decisione di armonizzazione ²².

Tre questioni meritano di essere segnalate.

a) *Il ruolo degli operatori di telecomunicazioni*. Gli operatori diventano soggetti di un sistema di sicurezza: rilevano, segnalano e, in fase di risposta (§ 6), possono essere chiamati a disattivare la SIM o il modulo di connessione su richiesta delle autorità. Il Piano richiede un quadro di governance nazionale tra autorità civili e militari, fornitori di apparati, proprietari delle torri e operatori, ma non ne indica i contenuti.

b) *La protezione dei dati e la riservatezza delle comunicazioni*. Il rilevamen-

²² Proposta di *Digital Networks Act*, COM(2026) 16, cui il Piano rinvia insieme alla proposta di revisione del regolamento sulla cibersicurezza, COM(2026) 11 (nota 22 del Piano). Mandato della Commissione alla CEPT sull'integrazione di funzioni di rilevamento (ISAC) nelle reti mobili nella banda 3,4-3,8 GHz, con bozza di relazione prevista per luglio 2027 e relazione finale per marzo 2028, in [https://cept.org/files/1412/ECC\(26\)042_Annex01_R1_Mandate%20to%20the%20CEPT%20on%20ISAC%20for%20drone%20detection.pdf](https://cept.org/files/1412/ECC(26)042_Annex01_R1_Mandate%20to%20the%20CEPT%20on%20ISAC%20for%20drone%20detection.pdf); il quadro da modificare è la decisione 2008/411/CE della Commissione, del 21 maggio 2008, relativa all'armonizzazione della banda di frequenze 3 400-3 800 MHz per i sistemi terrestri in grado di fornire servizi di comunicazioni elettroniche nella Comunità, in GU UE L 144 del 4 giugno 2008, come modificata, da ultimo, dalla decisione di esecuzione (UE) 2019/235 della Commissione, del 24 gennaio 2019, in GU UE L 37 dell'8 febbraio 2019.

to comportamentale delle SIM incide su dati di traffico e di localizzazione. Dovrà essere coordinato con il regolamento 2016/679, con la direttiva (UE) 2016/680 per i trattamenti a fini di polizia e soprattutto con la direttiva 2002/58/CE, che limita il trattamento dei dati di traffico e di ubicazione (artt. 5, 6 e 9) e ammette deroghe per finalità di sicurezza pubblica e di sicurezza nazionale solo alle condizioni dell'art. 15, par. 1. Il punto critico dipende dall'architettura del sistema, che il Piano non descrive. Se il rilevamento comportamentale richiedesse l'analisi automatizzata, in tempo reale, del traffico e degli spostamenti di tutte le utenze connesse, e non dei soli terminali già identificati come droni, si tratterebbe di un trattamento generalizzato e indifferenziato, che la Corte di giustizia ammette solo eccezionalmente, a fronte di una minaccia grave per la sicurezza nazionale, reale e attuale o prevedibile, per un tempo limitato e sotto il controllo di un giudice o di un'autorità indipendente; regole distinte, e non meno rigorose, valgono per la conservazione dei dati e per l'accesso delle autorità. La Corte ha inoltre precisato che la direttiva si applica anche quando il trattamento è imposto agli operatori dagli Stati per finalità di sicurezza nazionale²³. Diverso, e meno invasivo per gli altri utenti della rete, sarebbe un sistema limitato ai terminali pre-identificati come droni, secondo il modello di connessione che il Piano stesso prospetta. Il Comitato economico e sociale europeo, nel parere sul Piano, ha insistito proprio sulla proporzionalità e sul rispetto dei diritti fondamentali²⁴.

²³ Corte giust., 8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland e a.*; 6 ottobre 2020, cause riunite C-511/18, C-512/18 e C-520/18, *La Quadrature du Net e a.*, che si sofferma anche sull'analisi automatizzata e sulla raccolta in tempo reale dei dati di traffico e di ubicazione; 2 marzo 2021, causa C-746/18, *Prokuratuur*, sulle condizioni di accesso delle autorità a tali dati.

²⁴ Comitato economico e sociale europeo (CESE), parere TEN/883-EESC-2026 sul Piano d'azione, adottato nella sessione plenaria n. 607 del 15-16 luglio 2026 (relatore M. Hajnoš), in <https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/action-plan-drone-and-counter-drone-security>. Sul rapporto tra impiego pubblico dei droni e protezione dei dati personali, C. Della Giustina, *Droni. Il rapporto tra le pubbliche utilità e la privacy nell'esercizio degli unmanned vehicles*, Trieste, 2025, spec. p. 93 ss. sulla videosorveglianza nel diritto dell'Unione e p. 170 s. sulla frammentazione della tutela della riservatezza rispetto ai droni e sul caso *Carpenter v. United States*, 585 U.S. 296 (2018), relativo ai dati di localizzazione ricavati dalle celle telefoniche; J. Hovsha, D. O'Brien, *Drone Use Cases and their Privacy Impacts: A Taxonomy*, in *Tilburg Law Review*, vol. 27, n. 1, 2022, p. 60 ss., spec. p. 63 s. sull'identificabilità delle persone nei dati raccolti dai sensori dei droni e p. 65 ss. sulla valutazione d'impatto prevista dall'art. 35 del regolamento

c) *La compatibilità con la sicurezza aerea.* L'uso dello spettro a fini di rilevamento deve limitare le interferenze con l'aviazione, come il Piano stesso riconosce. È un vincolo che ritorna, con maggiore intensità, nelle misure di neutralizzazione.

6. – La terza parte del Piano parte da un'affermazione netta: la risposta operativa agli incidenti spetta agli Stati membri, per il suo legame con la sicurezza nazionale e la difesa, mentre l'Unione offre sostegno. Le misure sono numerose: un'iniziativa volontaria di dispiegamento di capacità antidrone per le infrastrutture critiche, avviata con un invito a manifestare interesse e fondata su una mappatura dei fabbisogni, un programma pilota di sviluppo congiunto e acquisti congiunti volontari; lo sviluppo di sistemi europei di comando e controllo basati sull'intelligenza artificiale, anche attraverso le *AI Gigafactories*; un'esercitazione annuale su scala europea, la cui prima edizione è prevista per l'autunno 2026; squadre di risposta rapida da esplorare entro il quarto trimestre 2026, cioè entro la fine dell'anno, come riserva dispiegabile su richiesta di uno Stato; il sostegno a Frontex. Una delle azioni, l'estensione della formazione delle forze di polizia alle misure di mitigazione e neutralizzazione, è già operativa: dal 1° al 5 giugno 2026 la rete europea per la sicurezza ad alto rischio (High Risk Security Network) ha tenuto in Portogallo, presso il centro di for-

2016/679; F. Granieri, *Navigating the Skies: A Cross-country Exploration of Drone Policies in Europe, USA and China, Unveiling Privacy and Cybersecurity Challenges*, in *Journal of Law, Market & Innovation*, 3 (2024), n. 2, p. 156 ss.; A. McKenna, *Privacy and Legal Enforcement*, in B.I. Scott (a cura di), *The Law of Unmanned Aircraft Systems*, cit., p. 161 ss., con riferimento agli ordinamenti del Regno Unito e del Kenya, spec. p. 168 ss. sull'impiego di droni per la sorveglianza da parte di soggetti pubblici e p. 171 ss. sul caso di Gatwick. Sui trattamenti di dati mediante droni da parte delle forze di polizia e sull'incerto confine tra regolamento 2016/679 e direttiva 2016/680, la cui clausola sulla salvaguardia contro le minacce alla sicurezza pubblica e la prevenzione delle stesse estende l'ambito della direttiva alla polizia predittiva e preventiva, E.Ö. Kurtpinar, *Privacy's Sky-High Battle: The Use of Unmanned Aircraft Systems for Law Enforcement in the European Union*, in *Journal of Intelligent & Robotic Systems*, 110 (2024), art. 99, spec. p. 3 ss. (anche sull'impiego di IMSI catcher a bordo dei droni) e p. 4 s., in <https://doi.org/10.1007/s10846-024-02071-w>; ivi, p. 9, sull'inapplicabilità della disciplina aeronautica europea ai droni di polizia, salvo che lo Stato se ne avvalga ai sensi dell'art. 2, par. 6, reg. 2018/1139. Sul piano tecnico, ETSI GR ISC 001 V1.1.1 (2025-03), *Integrated Sensing And Communications (ISAC); Use Cases and Deployment Scenarios*, Sophia Antipolis, marzo 2025, in https://www.etsi.org/deliver/etsi_gr/isc/001_099/001/01.01.01_60/gr_isc001v010101p.pdf. I contributi richiamati riguardano prevalentemente il trattamento di dati mediante droni e offrono perciò riferimenti sistematici: non risultano, a quanto consta, studi giuridici dedicati specificamente al rilevamento dei droni attraverso le reti mobili.

mazione della Guarda Nacional Republicana di Figueira da Foz, la terza edizione del proprio ciclo di formazione antidrone finanziato dall'Unione, con esercitazioni sull'uso di tecniche di mitigazione cinetiche e non cinetiche, dai disturbatori di frequenza ai proiettili. La formazione comune può così precedere il consolidamento delle basi giuridiche nazionali per l'impiego operativo di questi strumenti, che in molti Stati membri restano incerte (*infra*). Sul piano finanziario si segnalano l'invito da 250 milioni di euro dello strumento per la gestione delle frontiere e i visti, pubblicato nel dicembre 2025, i 169 milioni resi disponibili all'inizio del 2026 per l'acquisto di droni di sorveglianza e gli ulteriori 130 milioni messi a disposizione il 1° ottobre 2026, a valere sullo stesso strumento, per le capacità antidrone degli Stati membri: complessivamente, le risorse dei fondi per gli affari interni superano il mezzo miliardo di euro ²⁵.

Il paragrafo 4.6 del Piano è però il più importante per il giurista. Vi si riconosce che il quadro giuridico e operativo del contrasto ai droni, cioè dell'insieme di rilevamento, identificazione e neutralizzazione, è fortemente frammentato. La maggior parte degli Stati si affida a disposizioni sparse nella legislazione aeronautica, di polizia, di difesa e delle telecomunicazioni; pochi hanno una strategia nazionale integrata; alcuni non hanno alcuna regola. I gestori civili delle infrastrutture critiche non hanno, di norma, il potere di neutralizzare un drone, mentre le misure attive (disturbo, falsificazione del segnale, intervento cinetico) sono riservate a unità militari e di polizia specializzate, per i vincoli posti dalla disciplina dello spettro e della sicurezza aerea. Ne deriva un paradosso: chi può rilevare la minaccia non può rispondervi.

La risposta della Commissione si articola su due tempi. Nel breve periodo, una raccomandazione sul contrasto alle minacce dei droni per le forze di polizia e l'invito agli Stati a dotarsi di un quadro giuridico che consenta misure ef-

²⁵ Piano, § 4.5. Sui 130 milioni aggiuntivi, Commissione europea, Rappresentanza in Italia, La Commissione rafforza le capacità degli Stati membri nel settore dei droni e degli antidroni con 130 milioni di € aggiuntivi per potenziare la sicurezza delle frontiere, 5 ottobre 2026, in https://italy.representation.ec.europa.eu/notizie-ed-eventi/notizie/la-commissione-rafforza-le-capacita-degli-stati-membri-nel-settore-dei-droni-e-degli-antidroni-con-2026-10-05_it. Sulla formazione antidrone delle forze di polizia, Commissione europea, DG Migrazione e affari interni, EU High Risk Security Network organised a specialised training for law enforcement authorities, 23 giugno 2026, in https://home-affairs.ec.europa.eu/news/eu-high-risk-security-network-organised-specialised-training-law-enforcement-authorities-2026-06-23_en; la formazione è prevista dal Piano, § 2.2.2 e azioni chiave sulla preparazione (aggiornamento del ciclo formativo entro il secondo trimestre 2026, termine rispettato con la sessione di giugno).

ficaci, compreso l'abbattimento, e che metta in condizione i proprietari privati delle infrastrutture critiche di adottare le misure necessarie. Nel lungo periodo, uno studio di fattibilità su un quadro regolatorio europeo, da realizzare entro il 2030, con regole vincolanti e non vincolanti per autorità e operatori privati: requisiti minimi di prestazione dei sistemi, terminologia comune, monitoraggio integrato, segnalazione degli incidenti.

La difficoltà non è solo tecnica. In Italia il drone è un aeromobile ai sensi dell'art. 743 c. nav., e ogni intervento su un aeromobile in volo può incontrare, a seconda della condotta e delle circostanze, i limiti della sicurezza della navigazione aerea e del diritto penale, a cominciare dall'art. 432 c.p. sugli attentati alla sicurezza dei trasporti; l'uso di disturbatori di frequenza può urtare a sua volta contro il divieto di «arrecare disturbi o causare interferenze ai servizi di comunicazione elettronica» posto dall'art. 31, comma 2, del codice delle comunicazioni elettroniche (d.lgs. 1° agosto 2003, n. 259, nel testo sostituito dal d.lgs. 8 novembre 2021, n. 207) e assumere inoltre rilievo penale, a seconda delle condotte, dei servizi interessati e dei presupposti delle singole fattispecie, in relazione all'interruzione di un pubblico servizio (art. 340 c.p.) e, quando l'apparato impedisca anche comunicazioni telefoniche tra terzi, come quelle sulle reti mobili, all'installazione di apparecchiature a tal fine (art. 617-bis c.p.). Attribuire a un soggetto privato il potere di abbattere un aeromobile significa derogare a tali limiti, definire presupposti, modalità e responsabilità per i danni a terzi, e collocare quel potere rispetto al monopolio pubblico della forza. Sono scelte che spettano anzitutto al legislatore nazionale. L'Unione dispone di competenze in materia di cooperazione di polizia (artt. 87-89 TFUE), ma il mantenimento dell'ordine pubblico resta responsabilità degli Stati (art. 72 TFUE), e i titoli di competenza richiamati dal Piano non offrono, di per sé, una base immediata per attribuire ai privati un generale potere di neutralizzazione dei droni: il diritto dell'Unione può orientare queste scelte, e incidervi su specifiche basi giuridiche, ma difficilmente imporle. E, se un giorno queste scelte fossero compiute dall'Unione, richiederebbero comunque un atto legislativo, trattandosi a maggior ragione di elementi essenziali (v. *supra*, § 3). Per le forze di polizia, del resto, la base giuridica dell'impiego dei droni (art. 5, comma 3-sexies, d.l. n. 7 del 2015 e d.m. Interno 13 giugno 2022, che ha abrogato il precedente d.m. 29 aprile 2016) riguarda l'uso del mezzo, non il contrasto ai droni altrui ²⁶. In

²⁶ Per l'ordinamento italiano, M. Lamon, M. Bonazzi, *I droni a supporto della pubblica sicurezza*, in questa *Rivista*, 2021, p. 165 ss., spec. p. 176 s. sulla base giuridica dell'impiego da parte delle

manca di una disciplina organica e specifica del contrasto ai droni, l'intervento delle forze di polizia su un drone in volo, per esempio in occasione di grandi eventi, resta affidato alle cause di giustificazione. L'adempimento di un dovere (art. 51 c.p.) presuppone però una norma da cui il dovere discenda. L'uso legittimo delle armi o di altro mezzo di coazione fisica (art. 53 c.p.) è circoscritto alla necessità di respingere una violenza o di vincere una resistenza all'autorità e di impedire alcuni gravi delitti tassativamente indicati, tra cui la strage e il disastro aereo. Restano la legittima difesa (art. 52 c.p.), che presuppone il pericolo attuale di un'offesa ingiusta e la proporzione tra difesa e offesa, e lo stato di necessità (art. 54 c.p.), che richiede un pericolo attuale di danno grave alla persona. È una copertura costruita *a posteriori*, sul singolo fatto, inadatta a un'attività che dovrebbe essere pianificata; per il gestore privato, che non può invocare l'art. 53,

forze di polizia e p. 180 ss. sui sistemi di contrasto ai droni ostili, già allora privi di una disciplina adeguata a livello europeo e nazionale. Il d.m. 29 aprile 2016, esaminato dagli Autori, è stato poi abrogato dall'art. 11, comma 2, del d.m. 13 giugno 2022, Modalità di utilizzo da parte delle Forze di Polizia degli aeromobili a pilotaggio remoto, in GU n. 192 del 18 agosto 2022; sul quadro vigente, M. Mancini, *Droni e polizia locale: tra preclusione apparente e spazi di legittimità operativa*, in *Ethica Societas*, 16 febbraio 2026, in <https://www.ethicasocietas.it/droni-polizia-locale/>. Per un cenno ai sistemi counter-UAS in ambito militare, M. Lamon, *L'impiego dei droni militari*, in questa *Rivista*, 2024, p. 53 ss., spec. p. 55, nota 9, e p. 65, nota 39. Sui profili di *security* degli aeromobili senza equipaggio, A. Masutti, F. Tomasello, *Security Issues*, in B.I. Scott (a cura di), *The Law of Unmanned Aircraft Systems*, cit., p. 141 ss., spec. p. 144 s. sul rapporto tra *safety* e *security* negli artt. 4 e 88 del reg. 2018/1139, p. 145 ss. sui droni illeciti e sull'enforcement e p. 152 ss. sulle *measure counter-UAS* (piano d'azione EASA e mezzi tecnici del gruppo EUROCAE WG 115); v. anche Y. Morier, *Foreword to the Second Edition*, ivi, p. xlviii, che scompone i sistemi *counter-UAS* nelle fasi di rilevamento, identificazione, decisione ed eventuale neutralizzazione, osservando che le prime due sono comuni ai servizi di gestione del traffico UTM. In prospettiva comparata, U. Dieckert, *Regulatory Frameworks in Support of Counter-UAS*, in Joint Air Power Competence Centre (a cura di), *A Comprehensive Approach to Countering Unmanned Aircraft Systems*, Kalkar, 2021, p. 375 ss., spec. p. 378 s., 389 e 391 s., in <https://www.japcc.org/chapters/c-uas-regulatory-frameworks-in-support-of-counter-uas/>, che esclude l'uso di disturbatori da parte dei privati e propone «partenariati di sicurezza» con cui attribuire ai gestori di infrastrutture critiche poteri pubblici limitati. Sui limiti posti dal diritto internazionale aeronautico all'intercettazione dei droni non cooperativi, in particolare dall'art. 3 bis della Convenzione di Chicago, E.Ö. Kurtpinar, B.I. Scott, *The legality of countering potential threats posed by drones under international air law*, in 2024 International Conference on Unmanned Aircraft Systems (ICUAS), Chania, 2024, p. 347 ss.; sull'applicabilità dell'art. 3 bis agli aeromobili senza equipaggio impiegati in servizi civili, con il conseguente obbligo del pilota remoto di conformarsi agli ordini dello Stato sorvolato, L.F. Fiallos Pazmiño, *The International Civil Operations of Unmanned Aircraft Systems under Air Law*, Alphen aan den Rijn, 2021 (Aerospace Law and Policy Series, vol. 19), p. 59.

sembra ridursi a queste due ipotesi, di incerta applicazione a un drone di cui non sono ancora chiari intenzioni e carico.

Il confronto con gli Stati Uniti è istruttivo. Con il *National Defense Authorization Act* per il 2026 il Congresso ha esteso alle forze di polizia statali e locali poteri di contrasto ai droni prima riservati alle agenzie federali, subordinandoli a formazione e certificazione disciplinate da una norma provvisoria in vigore dal 1° luglio 2026; un disegno di legge presentato al Senato nell'aprile 2026 propone di estendere tali poteri al personale certificato dei gestori di infrastrutture critiche²⁷. In un ordinamento federale come quello statunitense la scelta può essere compiuta al centro; nell'Unione, nell'assetto attuale, la stessa scelta passa principalmente per ventisette legislatori nazionali. In Europa, del resto, la via legislativa nazionale è già stata percorsa: la Finlandia e, fuori

²⁷ National Defense Authorization Act for Fiscal Year 2026, Pub. L. 119-60, 18 dicembre 2025, tit. LXXXVI (*SAFER SKIES Act*), §§ 8601-8607, 139 Stat. 718, 1938-45, codificato in larga parte in 6 U.S.C. § 124n (§ 8602). Department of Justice e Department of Homeland Security, *Counter-UAS Authority for State, Local, Tribal, and Territorial Law Enforcement and Correctional Agencies*, interim final rule, in 91 Fed. Reg., n. 127, 6 luglio 2026, FR Doc. 2026-13609, in vigore dal 1° luglio 2026, in <https://www.federalregister.gov/documents/2026/07/06/2026-13609/counter-uas-authority-for-state-local-tribal-and-territorial-law-enforcement-and-correctional>; per una sintesi, Congressional Research Service, *Regulating State, Local, Tribal, and Territorial Law Enforcement Actions to Counter Unmanned Aircraft Systems (C-UAS)*, IF13279, 29 luglio 2026, in <https://www.everycrsreport.com/reports/IF13279.html>. Sul disegno di legge S. 4380 (*Critical Infrastructure Airspace Defense Act*), presentato il 22 aprile 2026, in <https://www.govinfo.gov/content/pkg/BILLS-119s4380is/xhtml/BILLS-119s4380is.html>; v. inoltre il comunicato del sen. Cotton, 23 aprile 2026, in <https://www.cotton.senate.gov/news/press-releases/cotton-introduces-bill-to-protect-critical-infrastructure-from-drones>. In Europa, il Regno Unito ha attribuito alla polizia poteri specifici sui droni con l'*Air Traffic Management and Unmanned Aircraft Act 2021*, il cui Schedule 8, par. 11, modifica la s. 93 del *Police Act 1997* per consentire l'interferenza con i beni e con le comunicazioni radio dei droni impiegati nella commissione di determinati reati, ed estende le autorità competenti ad autorizzarla al capo della Civil Nuclear Constabulary e alla dirigenza degli istituti penitenziari: G. Leloudas, *United Kingdom*, in J. Hartmann, B.I. Scott, S. Truxal, A. Bertolini, A. Masutti (a cura di), *Civil Regulation of Autonomous Unmanned Aircraft Systems in Europe*, Cheltenham, 2024, p. 274 ss., spec. p. 299 ss. In Finlandia, secondo la ricostruzione di M.T. Huttunen, il *Police Act* consente agli agenti di sequestrare i droni o di interromperne il volo, anche monitorando il traffico radio e impiegando dispositivi tecnici per abbatterli: M.T. Huttunen, *Finland*, ivi, p. 137 ss., spec. p. 150 e p. 155 s., ove si osserva che, spettando la sicurezza nazionale agli Stati (art. 4, par. 2, TUE), l'intervento dell'Unione resta concentrato sulla *security* aeroportuale e che il solo potere di polizia non basta a fronteggiare le minacce. Sulla proposta del Governo finlandese del settembre 2026, che estenderebbe i poteri di intercettazione a tutti i veicoli senza equipaggio, Yle, 15 settembre 2026, in <https://yle.fi/a/74-20246405>.

dall'Unione, il Regno Unito (nel 2021) hanno attribuito alla polizia poteri espressi di interferenza con i droni, e il Governo finlandese ha proposto nel settembre 2026 di ampliarli. L'orizzonte del 2030 rischia di essere troppo lungo rispetto alla velocità della minaccia che il Piano descrive.

Un quadro europeo, se e quando verrà, dovrebbe almeno distinguere tra rilevamento, che può essere ampiamente consentito nel rispetto della disciplina dei dati personali, delle comunicazioni e dello spettro, e mitigazione, da riservare a soggetti autorizzati secondo una scala graduata di misure; prevedere la certificazione dei sistemi, sulla base dei criteri di sicurezza aerea che il Piano affida all'EASA; disciplinare la formazione del personale, la responsabilità per i danni e il controllo successivo sull'uso dei poteri.

Vi è infine un profilo che interessa da vicino il diritto dei trasporti. Gli aeroporti e i terminal portuali sono in larga parte gestiti in regime concessorio (art. 704 c. nav.; art. 18 della legge n. 84 del 1994). Se una parte degli oneri di rilevamento e di risposta sarà posta a carico dei gestori, conviene distinguere. Vi sono anzitutto i costi: l'acquisto e l'aggiornamento dei sistemi, il personale e la sua formazione, la manutenzione e il coordinamento con i servizi del traffico aereo e con le forze di polizia. Bisognerà stabilire chi li sopporti, se e come incidano sull'equilibrio economico-finanziario della concessione e se possano essere recuperati attraverso i diritti aeroportuali e portuali. Vi sono poi le responsabilità, che mutano con la natura dell'attività. Per il mancato rilevamento o per una segnalazione errata si risponde della violazione di un obbligo di sorveglianza. Per i danni causati da un intervento materiale sul drone la responsabilità presuppone un potere che solo la legge può attribuire. Soprattutto, occorrerà stabilire chi eserciti il controllo²⁸. La protezione dello scalo da una minaccia ibrida è una

²⁸ Il precedente più prossimo è l'affidamento in concessione ai gestori aeroportuali dei servizi di controllo di sicurezza che non richiedono l'impiego di personale delle forze di polizia, disposto dall'art. 5 del d.l. 18 gennaio 1992, n. 9, convertito, con modificazioni, dalla l. 28 febbraio 1992, n. 217, e attuato con il d.m. 29 gennaio 1999, n. 85, Regolamento recante norme di attuazione dell'articolo 5 del decreto-legge 18 gennaio 1992, n. 9, convertito, con modificazioni, dalla legge 28 febbraio 1992, n. 217, in materia di affidamento in concessione dei servizi di sicurezza, in GU n. 77 del 2 aprile 1999, poi modificato dal d.m. 13 settembre 2002, n. 263. Il gestore esegue i controlli, mentre la definizione delle regole, la vigilanza e l'impiego della forza restano all'amministrazione e alle forze di polizia; i costi sono recuperati con corrispettivi a carico dei passeggeri e/o dei vettori (art. 5, comma 3, del d.l. n. 9 del 1992), posti a carico dell'utenza che effettivamente usufruisce del servizio «a copertura dei costi e quale corrispettivo del servizio reso» (art. 8 del d.m. n. 85 del 1999). Il corrispettivo per il controllo di sicurezza sul passeggero e sul bagaglio a mano rientra

funzione pubblica: il gestore può esserne il braccio operativo, ma la regia deve restare all'amministrazione, cui spetta definire gli standard, verificarne il rispetto e decidere in ultima istanza l'uso dei mezzi coercitivi. Nei porti, del resto, è già un'autorità pubblica a guidare l'integrazione dei droni nelle attività di *security*: l'Autorità di sistema portuale del Mare di Sicilia occidentale ha avviato, con un protocollo d'intesa triennale, l'iter per l'istituzione di uno spazio aereo U-space nel porto di Palermo e la sperimentazione dei droni per il monitoraggio delle infrastrutture e il supporto alla *security*²⁹. L'iniziativa riguarda l'impiego dei droni autorizzati, non il contrasto a quelli ostili, ma ne prepara la cornice: nello U-space i droni devono essere identificati in rete (v. *supra*, nota 12), sicché quelli che non lo sono possono essere riconosciuti più facilmente.

7. – L'ultima parte del Piano riguarda la prontezza difensiva. I droni e i sistemi antidrone sono un'area di capacità prioritaria concordata dagli Stati membri nell'ambito della *Defence Readiness Roadmap 2030*, e il Piano li collega alla *European Drone Defence Initiative* e all'iniziativa *Eastern Flank Watch*. Le risorse indicate sono rilevanti: un miliardo di euro già destinato dal Fondo europeo per la difesa e dai programmi precedenti a ricerca e sviluppo sui droni, 200 milioni previsti per i prossimi due anni, gli acquisti finanziati con lo strumento SAFE istituito dal regolamento (UE) 2025/1106, il sostegno alla produzione industriale tramite il programma EDIP³⁰. A ciò si aggiungono la *Drone Alliance* con l'Ucraina, per mettere a frutto l'esperienza maturata sul

oggi tra i corrispettivi regolati dai modelli dell'Autorità di regolazione dei trasporti: delibera n. 38/2023 del 9 marzo 2023, Allegato A, in https://www.autorita-trasporti.it/wp-content/uploads/2023/03/All.-A-delibera-n.-38_2023_signed.pdf. Per la *security* portuale, v. *supra*, nota 15.

²⁹ Autorità di sistema portuale del Mare di Sicilia occidentale, *Porto di Palermo: avviato l'iter per l'utilizzo dei droni*, comunicato del 23 giugno 2026, in <https://www.adspalermo.it/news/porto-di-palermo-avviato-liter-lutilizzo-dei-droni>. Il protocollo, sottoscritto il 25 maggio 2026 con STRADA Ai – STRADA Artificial Intelligence S.r.l., prevede la mappatura delle zone geografiche UAS dell'area portuale e almeno un progetto pilota.

³⁰ Regolamento (UE) 2025/1106 del Consiglio, del 27 maggio 2025, che istituisce lo strumento di azione per la sicurezza dell'Europa (SAFE) mediante il rafforzamento dell'industria europea della difesa, in GU UE L del 28 maggio 2025; regolamento (UE) 2025/2643 del Parlamento europeo e del Consiglio, del 16 dicembre 2025, che istituisce il programma per l'industria europea della difesa e istituisce un quadro di misure per garantire la disponibilità e l'approvvigionamento tempestivi dei prodotti della difesa (regolamento EDIP), in GU UE L del 29 dicembre 2025 (il Piano cita ancora la proposta COM(2024) 150 final). Le cifre sono tratte dal § 5 del Piano.

campo di battaglia, e il forum industriale D-TECT, che riunisce l'ecosistema civile e militare dei produttori. Il forum, previsto dal Piano per il secondo trimestre 2026, ha in programma, con alcuni mesi di ritardo, la sua riunione inaugurale per l'11 novembre 2026 ³¹.

Dal punto di vista giuridico, la dimensione della difesa pone soprattutto un problema di confini. Il regolamento 2018/1139 non si applica agli aeromobili quando svolgono attività o servizi militari, doganali, di polizia, di ricerca e soccorso, antincendio, di controllo delle frontiere, di guardia costiera o analoghi, sotto il controllo e la responsabilità di uno Stato membro e nell'interesse pubblico – art. 2, par. 3, lett. a) – e il quadro del 2019 è costruito su questa distinzione. Il Piano, invece, ragiona per capacità *dual use*: sistemi di rilevamento «civili per progettazione» ma integrabili nella difesa aerea, comandi e controllo comuni, standard condivisi tra EASA, Agenzia europea per la difesa e NATO. Lo stesso confine attraversa la disciplina dell'intelligenza artificiale, cui il Piano affida l'allerta precoce sulle reti mobili e i sistemi di comando e controllo. Il regolamento (UE) 2024/1689 esclude dal proprio ambito i sistemi immessi sul mercato o utilizzati esclusivamente per scopi militari, di difesa o di sicurezza nazionale (art. 2, par. 3), ma vi riconduce quelli impiegati per finalità civili o di contrasto, anche se sviluppati per la difesa, e qualifica ad alto rischio, tra gli altri, i sistemi usati come componenti di sicurezza nella gestione delle infrastrutture digitali critiche e alcuni sistemi impiegati dalle autorità di contrasto (allegato III, punti 2 e 6) ³². Un sistema «civile per progettazione» ma integrato nella difesa aerea può dunque ricadere ora dentro ora fuori dal regolamento, secondo l'uso che ne viene fatto. La sinergia è comprensibile, ma spostata verso l'area della sicurezza e della difesa una porzione crescente di regole che riguardano anche l'uso civile dello spazio aereo a bassa quota. Il Comitato economico e sociale europeo ha sottolineato che la sicurezza della navigazione aerea deve restare la priorità assoluta nel-

³¹ Commissione europea, Drone Tech for Countering Threats (D-TECT) Forum, in <https://digital-strategy.ec.europa.eu/en/policies/d-tect-forum>; per la data dell'incontro inaugurale, EU Agenda, 10 agosto 2026, in <https://euagenda.eu/news/932458>.

³² Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale, in GU UE L del 12 luglio 2024, spec. art. 2, par. 3, considerando 24 e allegato III, punti 2 e 6. L'applicazione degli obblighi relativi ai sistemi ad alto rischio dell'allegato III è stata differita al 2 dicembre 2027 dal regolamento (UE) 2026/1744 del Parlamento europeo e del Consiglio, dell'8 luglio 2026, in GU UE L del 24 luglio 2026, che modifica anche il regolamento 2018/1139.

la progettazione e nell'uso dei sistemi antidrone, a tutela dell'integrità del sistema di gestione del traffico aereo³³. È un richiamo opportuno: i sistemi che disturbano o neutralizzano un drone operano nello stesso spazio del traffico con equipaggio e possono interferire con frequenze e sistemi impiegati dall'aviazione.

Il Piano affida all'EASA, quale autorità competente per la sicurezza aerea, la definizione dei criteri che i sistemi antidrone dovranno rispettare. È la scelta corretta, perché consente di integrare la sicurezza della navigazione aerea nella definizione dei requisiti dei sistemi, che altrimenti sarebbe guidata solo da esigenze di efficacia operativa. Resta da vedere se i criteri saranno vincolanti, e per quali utilizzatori. Le esclusioni dell'art. 2, par. 3, del regolamento 2018/1139 non consentono di considerare automaticamente sottratto alla disciplina europea ogni sistema antidrone impiegato da autorità militari o di polizia: occorrerà distinguere le diverse componenti del sistema, che possono comprendere anche droni intercettori, l'attività svolta e la base giuridica degli eventuali requisiti vincolanti.

Il Piano non può essere letto isolatamente. È l'ultimo tassello di una sequenza che, dall'insediamento della seconda Commissione von der Leyen, ha spostato il baricentro dell'azione dell'Unione verso la sicurezza e la difesa: l'istituzione, per la prima volta, di un commissario per la difesa e lo spazio; il Libro bianco sulla difesa europea e il piano *ReArm Europe – Readiness 2030* del marzo 2025; lo strumento SAFE, adottato dal solo Consiglio sulla base dell'art. 122 TFUE, cioè di una clausola pensata per le difficoltà economiche gravi, con l'esclusione del Parlamento europeo, che lo ha impugnato; la *Defence Readiness Roadmap 2030*³⁴. In questo disegno la politica dei trasporti e quella del

³³ CESE, parere TEN/883, cit., punti chiave.

³⁴ Commissione europea e Alto rappresentante, *Libro bianco sulla difesa europea – Prontezza 2030*, JOIN(2025) 120 final, 19 marzo 2025; regolamento (UE) 2025/1106, cit. (SAFE), adottato sulla base dell'art. 122 TFUE. Il Parlamento europeo ne ha chiesto l'annullamento con ricorso proposto il 20 agosto 2025, causa C-560/25, Parlamento c. Consiglio (GU C, C/2025/5209, 6 ottobre 2025), tuttora pendente, sostenendo che la base giuridica corretta fosse l'art. 173 TFUE e lamentando un difetto di motivazione della scelta (art. 296 TFUE). In dottrina, criticamente, M. Dani, A.J. Menéndez Menéndez, *The EU's (not so) cheap talk on defence*, in *European Law Open*, 4 (2025), n. 3, p. 425 ss.; M. Leson, *Moving towards a SAFE Defense Policy in Europe: Emergency Powers Move into the Realm of Security and Defense Policy*, in *Verfassungsblog*, 12 settembre 2025, in <https://verfassungsblog.de/safeact-eu-defense/>; M. Genovese, *Rearming Europe Through Article 122 TFEU: 'Defence Readiness', Emergency Governance and Constitutional Change*, in *Croatian Yearbook of European Law and Policy*, 22 (2026), online first, in <https://www.cypel.com/index.php/cypel/article/view/612>; P. Dermine, *Funding Europe's Defence: A First Take On the Commission's ReArm*

mercato interno diventano veicoli di una politica di sicurezza e, sempre più, di difesa: è questa la svolta securitaria e bellicista in cui il Piano si colloca. «Bellicista» esprime qui un giudizio dichiaratamente politico, non giuridico né sulle intenzioni. Indica la direzione che la Commissione ha impresso all'integrazione sotto la pressione della guerra, estendendola a poteri tradizionalmente riservati agli Stati, come la difesa e la sicurezza. È una lettura che trova riscontro tanto nella dottrina quanto nel dibattito geopolitico³⁵. Le sue conseguenze giuridiche sono invece quelle esaminate in queste pagine: l'uso di basi giuridi-

Europe Plan, in *Verfassungsblog*, 5 marzo 2025, in <https://verfassungsblog.de/rearm-europe-law/>; E. Chiti, *Il rafforzamento della difesa europea*, in *Giorn. dir. amm.*, 2025, n. 2, p. 145 ss.; Editorial Comments, *ReArm Europe/Readiness 2030: European defence in times of war*, in *Common Market Law Review*, 62 (2025), n. 4, p. 1019 ss.; A. Somma, *L'Unione europea nel sistema di guerra: il conflitto russo ucraino e le evoluzioni del capitalismo*, in *Costituzionalismo.it*, 2025, n. 2, in <https://www.-costituzionalismo.it/lunione-europea-nel-sistema-di-guerra-il-conflitto-russo-ucraino-e-le-evoluzioni-del-capitalismo/>. Sull'uso espansivo dell'art. 122 TFUE, P. Leino-Sandberg, M. Ruffert, *Next Generation EU and Its Constitutional Ramifications: A Critical Assessment*, in *Common Market Law Review*, 59 (2022), n. 2, p. 433 ss.; in senso diverso, per una lettura dell'art. 122, par. 1, TFUE come base di una competenza di politica economica non limitata alle emergenze, M. Chamon, *The Non-Emergency Economic Policy Competence in Article 122(1) TFEU*, *ivi*, 61 (2024), n. 6, p. 1501 ss.; B. de Witte, *EU Emergency Law and Its Impact on the EU Legal Order*, *ivi*, 59 (2022), n. 1, p. 3 ss. Sull'integrazione «bellicista» e sulla svolta geoeconomica della politica industriale della difesa, P. Genschel, *Bellicist Integration? The War in Ukraine, the European Union and Core State Powers*, in *Journal of European Public Policy*, 29 (2022), n. 12, p. 1885 ss.; D. Fiott, *From Liberalisation to Industrial Policy: Towards a Geoeconomic Turn in the European Defence Market?*, in *Journal of Common Market Studies*, 62 (2024), n. 4, p. 1012 ss. Sull'imperativo di «security and resilience» che, dopo l'aggressione russa all'Ucraina, il Master Plan europeo della gestione del traffico aereo del 2025 estende alla navigazione aerea, ridefinendo la cooperazione civile-militare, F. Franchina, *European Union Air Navigation Services and Digitalization*, in M.P. Rizzo, F. Franchina (a cura di), *Drones in the Digital European Sky*, *cit.*, p. 221 ss., spec. p. 234 s.; dello stesso A., *Il «Digital European Sky»*, in questa *Rivista*, 2025, suppl. *ATM, Drones and Digitalization, Artificial Intelligence and New Technologies for Environment*, p. 37 ss., spec. p. 54, sull'interoperabilità civile-militare e sulle tecnologie a duplice uso nel progetto di cielo digitale europeo. La *Defence Readiness Roadmap 2030* è richiamata ai §§ 1 e 5 del Piano.

³⁵ Oltre agli scritti citati *supra*, nota 34, v. G. Guerra, *«ReArm Europe» e dintorni. Sulla svolta militarista e bellicista dell'Unione europea*, in *DPCE Online*, 2025, n. 4, p. 1641 ss. Nel dibattito geopolitico, sulla debole base giuridica del piano di riarmo promosso dalla Commissione, fondato sull'art. 122 TFUE con l'esclusione del Parlamento europeo, v. R. Ferrari Zumbini, *La trappola di Bruxelles o dell'emoziocrazia*, in *Limes*, 2025, n. 3, p. 135 ss., spec. p. 136. Sul riarmo deciso in tempi rapidi contro una minaccia valutata in modo sommario, e a scapito della risposta alla guerra ibrida, v. H. Staal, *Il continente fa ricchi i mercanti d'armi*, in *Internazionale*, 14 marzo 2025, n. 1605, p. 18. Sulla minaccia dei droni russi sul fianco orientale della NATO, v. S. Sierakowski, *I droni russi*

che nate per altri fini e la marginalità del Parlamento europeo.

Il testo del Piano ne porta i segni. La formula secondo cui una minaccia contro uno Stato membro è una minaccia contro l'Unione nel suo insieme richiama, nel lessico, la clausola di difesa reciproca dell'art. 42, par. 7, TUE e l'art. 5 del Trattato del Nord Atlantico, ma è usata per giustificare misure che riguardano anche il drone del fotografo amatoriale. Accanto ai fondi per la sicurezza interna, le misure del Piano e lo sviluppo industriale si appoggiano a strumenti della difesa: il Fondo europeo per la difesa, l'EDIP, SAFE e, per il periodo successivo al 2027, l'ambito di intervento «Resilienza e sicurezza, industria della difesa e spazio» previsto dalla proposta di Fondo europeo per la competitività (COM(2025) 555 final, 16 luglio 2025, art. 1, par. 2, lett. d). I sistemi di rilevamento sono «civili per progettazione», ma concepiti per integrarsi nella sorveglianza aerea militare. Per la componente industriale e di difesa, il modello dichiarato è l'esperienza maturata sul campo di battaglia ucraino. Persino l'agenda «positiva» sui droni, cioè la crescita del mercato, è presentata come conseguenza della sicurezza, non come valore autonomo. E il registro dell'urgenza, che ricorre in tutto il documento, comprime i tempi della deliberazione: il Piano opera per comunicazioni, atti di esecuzione, iniziative volontarie e inviti a manifestare interesse, cioè per canali che sfuggono in larga parte alla procedura legislativa ordinaria.

I costi di questa svolta sono almeno quattro.

i) *Un costo democratico*. Le scelte più incisive passano per atti della Commissione e per strumenti del Consiglio, con un ruolo marginale del Parlamento europeo e dei parlamenti nazionali. Se adottata, come propone l'EASA, la riduzione a 100 g della soglia di registrazione, con verifica dell'identità, estenderà e renderà più uniformi gli obblighi gravanti su un'ampia platea di operatori, anche ricreativi, senza una nuova deliberazione legislativa sul contenuto specifico delle misure, con un evidente problema di equilibrio istituzionale e di riserva al legislatore degli elementi essenziali (v. *supra*, § 3).

ii) *Un costo per i diritti*. Registrazione generalizzata, identificazione remota, rilevamento comportamentale delle SIM e subordinazione della connettività alla pre-identificazione compongono un'infrastruttura di sorveglianza dello spazio aereo a bassa quota che, una volta costruita, potrà essere usata per finalità diverse da quelle originarie. Un termine di confronto è offerto dal parame-

sfidano la Nato e Trump, ivi, 19 settembre 2025, n. 1632, p. 34.

tro che la Corte di giustizia ha elaborato per i dati di traffico e di ubicazione: un trattamento generalizzato è ammesso solo per finalità delimitate, per un tempo definito e sotto un controllo indipendente ³⁶. Non a caso il Comitato economico e sociale europeo ha richiamato la necessità che ogni misura resti proporzionata e soggetta a responsabilità democratica ³⁷.

iii) *Un costo per la logica della disciplina aeronautica*. Nel quadro del 2019, gli obblighi di un drone di 120 g dipendono dai rischi che presenta in concreto, per la sicurezza o per la riservatezza: la registrazione, per esempio, è legata all'energia cinetica che può trasmettere in caso di impatto e alla presenza di sensori in grado di raccogliere dati personali, salvo che si tratti di un giocattolo. Nel paradigma della *security* lo stesso drone sarebbe assoggettato in via generale alla registrazione dell'operatore e all'identificazione remota, in funzione della sua tracciabilità: non più perché pericoloso, ma perché da verificare. Il nuovo regime estende e uniforma gli obblighi per una fascia di apparecchi oggi soggetta a regole differenziate. L'operatore cittadino è chiamato a rendere costantemente verificabile la propria legittimità, con il rischio che la mancata identificazione sia trattata, nella prassi operativa, come indice di pericolosità anziché come anomalia da accertare.

iv) *Un costo per l'autonomia del civile*. Le sinergie civili-militari e gli standard comuni tra EASA, Agenzia europea per la difesa e NATO rischiano di attrarre verso la logica militare regole e tecnologie che riguardano anzitutto usi civili: la logistica, l'agricoltura, l'ispezione delle infrastrutture, il soccorso.

Non si tratta di negare la minaccia: le incursioni di droni russi nello spazio aereo di Stati membri, come in Polonia nel settembre 2025 e in Romania nel maggio 2026, sono accertate, e le chiusure di aeroporti seguite agli avvistamenti dell'autunno 2025 hanno mostrato la vulnerabilità delle infrastrutture, anche se in molti casi né la presenza dei droni né la loro provenienza sono state chiarite ³⁸.

³⁶ V. *supra*, nota 23.

³⁷ CESE, parere TEN/883, cit., punti chiave, che richiama proporzionalità, diritti fondamentali, protezione dei dati, certezza del diritto e responsabilità democratica.

³⁸ Sull'incursione in Polonia, v. *supra*, nota 2. Per la Romania, Unione europea, *EU Statement on the reckless violation of the EU's airspace by Russia*, 3 giugno 2026, in https://www.eeas.europa.eu/delegations/council-europe/eu-statement-reckless-violation-eu%E2%80%99s-airspace-russia_en. Per l'aeroporto di Copenaghen, Københavns Politi, *Efterforskningen af droneobservationer over Københavns Lufthavn er indstillet*, 25 giugno 2026, in <https://politi.dk/koebenhavns-politi/nyhedsliste/efterforskningen-af-droneobservationer-over-koebenhavns-lufthavn-er-indstillet/2026/06/25>; nella conferenza stampa dello stesso giorno la

Né si contesta che una risposta europea coordinata sia preferibile a ventisette risposte disordinate. La critica riguarda la *misura*: la sicurezza è un interesse da bilanciare, non il principio che ordina e subordina tutti gli altri. Per restituirle una misura servirebbero alcuni accorgimenti che il Piano non prevede: una valutazione d'impatto delle misure sui diritti fondamentali e sugli operatori legittimi; clausole di riesame e di decadenza per le misure giustificate dall'emergenza; un coinvolgimento effettivo del Parlamento europeo nelle scelte che toccano le libertà dei cittadini; la separazione, anche organizzativa, tra la disciplina della sicurezza dell'aviazione civile, affidata all'EASA, e le esigenze della difesa.

8. – Il Piano d'azione del febbraio 2026 non crea un diritto europeo della sicurezza dei droni, ma ne disegna l'architettura, e la disegna sotto il segno della minaccia. Il suo contenuto può essere ricondotto a tre livelli, che corrispondono ad altrettante modalità d'intervento dell'Unione.

Il primo è la *regolazione*, dove l'Unione dispone di un titolo settoriale: la registrazione e l'identificazione remota dei droni a partire da 100 g e la verifica dell'identità degli operatori, proposte dal parere EASA e non ancora adottate, i requisiti di progettazione, la sicurezza informatica dei prodotti, lo spettro per il rilevamento. Qui il Piano si traduce in tempi brevi in proposte normative, come mostra il parere EASA n. 06/2026, adottato appena sette mesi dopo la comunicazione.

Il secondo è il *coordinamento*, dove prevalgono le responsabilità operative degli Stati, anche quando, come per la resilienza dei soggetti critici, esiste già una disciplina europea vincolante: orientamenti sulla resilienza delle infrastrutture critiche, *stress test* volontari, raccomandazioni alle forze di polizia, acquisti congiunti, esercitazioni, squadre di risposta rapida, coordinatori nazionali. La sua efficacia dipende in misura decisiva dalla volontà degli Stati e dalla capacità della Commissione di trasformare la «co-ownership» in un metodo.

polizia ha concluso che la presenza di droni sull'aeroporto il 22 settembre 2025 non può essere né provata né esclusa, mentre le Forze armate danesi hanno ritenuto che in più occasioni vi siano stati droni sul territorio danese: Altinget, *Politiet kan ikke bevise droneaktivitet ved Københavns Lufthavn*, 25 giugno 2026, in <https://www.altinget.dk/forsvar/artikel/politiet-kan-ikke-bevise-droneaktivitet-ved-koebenhavns-lufthavn>. Per un quadro degli episodi del 2025 e dell'esito delle indagini, anche sull'assenza di prove ufficiali circa la responsabilità russa negli avvistamenti presso gli aeroporti, Euronews, *Fact-checking Europe's 'drone problem': Why are airports closing over drone sightings?*, 20 novembre 2025, in <https://www.euronews.com/2025/11/20/fact-checking-europes-drone-problem-why-are-airports-shuttering-over-drone-sightings>.

Il terzo è il *finanziamento industriale e della difesa*, che mobilita le risorse più consistenti e lega la sicurezza civile alla prontezza militare.

Tra il primo e il secondo livello resta scoperto il punto decisivo: chi possa neutralizzare un drone, con quali mezzi e con quali responsabilità. Il Piano ha il merito di dichiarare con franchezza la lacuna, ma la affida a uno studio di fattibilità con orizzonte al 2030. Nel frattempo, la risposta dipenderà dai legislatori nazionali.

Accanto alla svolta securitaria, altri tre profili critici emergono dall'analisi. Il primo è il mancato raccordo del Piano con la disciplina della *security* aeroportuale e portuale, che pure è il luogo naturale in cui integrare la minaccia dei droni per i nodi di trasporto. Il secondo è il bilanciamento con i diritti fondamentali, che la registrazione con verifica dell'identità e il rilevamento basato sulle reti mobili rendono tutt'altro che teorico. Il terzo è il rischio che la *security* gravi soprattutto sugli operatori legittimi, che registrano e identificano i propri droni, lasciando sostanzialmente invariata la posizione di chi opera in modo ostile: un rischio che un sistema di rilevamento efficace, capace di sfruttare la registrazione come filtro, può contribuire a ridurre.

Per l'Italia, il Piano pone tre compiti: adeguare l'ordinamento nazionale alle modifiche dei regolamenti 2019/945 e 2019/947, una volta adottate, aggiornando il regolamento UAS-IT e la pubblicazione delle zone geografiche; dotarsi di una disciplina organica del contrasto ai droni, che definisca soggetti, presupposti e limiti dei poteri di neutralizzazione; designare il coordinatore nazionale per la sicurezza dei droni richiesto dalla Commissione, che non risulta ancora nominato. Nel farlo, si dovrà considerare che una parte rilevante delle infrastrutture da proteggere è gestita da concessionari: la loro collaborazione è indispensabile, ma vanno tenuti distinti tre piani: la titolarità della funzione di protezione e la determinazione dei suoi limiti, che devono restare pubbliche; gli obblighi di protezione e, entro un quadro definito dalla legge, i singoli interventi materiali, che possono spettare ai gestori; il controllo sull'esercizio di tali attività, anch'esso pubblico, e la conseguente ripartizione delle responsabilità.

Resta, sullo sfondo, la questione più generale. Il quadro del 2019 era nato per integrare i droni nello spazio aereo come strumenti di innovazione civile, secondo una logica di proporzionalità al rischio. Il Piano del 2026 li ricolloca nello spazio della minaccia e della difesa, in coerenza con una Commissione che ha posto il riarmo e la prontezza militare al centro della propria azione (§

7). Il giurista dei trasporti non può limitarsi a registrare il cambiamento: deve chiedere che la sicurezza resti un interesse da bilanciare, sottoposto a controllo democratico e a verifica di proporzionalità, e che lo spazio aereo a bassa quota non diventi, per gradi e senza un vero dibattito, uno spazio militarizzato.

Abstract

Con il Piano d'azione sulla sicurezza dei droni e antidrone (COM(2026) 81 final, 11 febbraio 2026) la Commissione sposta la politica europea sui droni dal paradigma della *safety*, su cui è costruito il quadro del 2019, a quello della *security*, che da finalità concorrente diventa finalità prevalente. Il commento legge questo passaggio con preoccupazione, come espressione della più generale svolta securitaria e bellicista che caratterizza la seconda Commissione von der Leyen, e sostiene che il Piano segue nel complesso la geometria delle competenze dell'Unione, pur forzandone talvolta i confini: prefigura interventi vincolanti dove l'Unione dispone già di una base settoriale (registrazione e identificazione remota, requisiti di prodotto, spettro radio), privilegia il coordinamento dove prevalgono le responsabilità operative degli Stati (protezione delle infrastrutture critiche, risposta operativa) e affida a uno studio di fattibilità con orizzonte al 2030 il nodo più delicato, cioè l'attribuzione dei poteri di neutralizzazione. Sono esaminati il pacchetto di revisione dei regolamenti (UE) 2019/945 e 2019/947 delineato dal parere EASA n. 06/2026, il ruolo delle reti 5G nel rilevamento, il rapporto con la disciplina della *security* aeroportuale e portuale, che il Piano non richiama, e le ricadute sui gestori di infrastrutture di trasporto in regime concessorio.

With the Action Plan on Drone and Counter-Drone Security (COM(2026) 81 final, 11 February 2026), the Commission moves EU drone policy from the safety paradigm underpinning the 2019 framework to a security paradigm, turning security from a concurrent into a prevailing aim. This comment views this shift with concern, as an expression of the broader securitarian and militarising turn of the second von der Leyen Commission, and argues that the Plan broadly follows the map of EU competences, while at times stretching its boundaries: it foreshadows binding measures where the Union already has a sectoral legal basis (registration and remote identification, product requirements, radio spectrum), it favours coordination where Member States' operational responsibilities prevail (critical infrastructure protection, operational response), and it leaves to a feasibility study with a 2030 horizon the most sensitive issue, namely the allocation of neutralisation powers. The comment examines the revision of Regulations (EU) 2019/945 and 2019/947 outlined in EASA Opinion No 06/2026, the role of 5G networks in detection, the relationship with aviation and port security law, which the Plan does not address, and the implications for concession-holding transport infrastructure operators.