LIBRO BLANCO SOBRE AUTOMATIZACIÓN UAS

PROYECTO FINANCIADO POR PTR2022-001299

FINANCIADO POR CONVOCATORIA PLATAFORMAS TECNOLÓGICAS Y DE INNOVACIÓN 2022

Índice

Control de cambios

Autores	Versión	Fecha	Modificaciones
Líderes de sección: **CATEC** Antidio Viguria Jiménez **AIRBUS** Francisco Javier Ramos Salas **Universidad de Alicante. AEDAE** Yolanda Bustos Moreno **Participantes GT Autonomía de la PAE** **ABIONICA** Antonio Bedmar **AERTEC** Sara Bellido **AHYRES** Juan Carlos Marín **AIMPLAS** Antonio Penadés **AIRBUS** Juan Manuel Jiménez **BCN Drone Center** Ernest Millares **Bufete Mas y Calvet** Efrén Díaz **CATUAV** Jordi Salvador **EURECAT** Anton Gorostiaga **ENAIRE** Daniel García-Monteavaro Raquel Moldes Marc Olmo **GMV** Almudena Sánchez Jorge Ocón Daniel Montero Yéboles **Grupo Álava** Jorge Pina **ITG** Enrique Ventas Marco A. González **NET2FLY** Claudia Romeo **TECNALIA** Javier Coleto **TEKNIKER** Oscar Gonzalo **TELESPAZIO** Nahum Zaera **UAH** Daniel Meziat	V1.0	11/04/2025	Primera versión para publicar.

UC3M Jesús García Herrero Luis Enrique Moreno José Manuel Molina **UPCT** María Dolores Cano **UPM** Juan José Morillas **UPV** Israel Quintanilla Juan Alberto Martínez Jordi Vidal **URJC** Raúl Celis **US** Aníbal Ollero Cristina María Arévalo **Supervisión PAE:** Andrés Catalán **Coordinación:** **CATEC** Antidio Viguria Jiménez			

Introducción

El sector UAS se encuentra actualmente en un punto crucial en el que cada vez se está desarrollando servicios que requieren operaciones más complejas y además se busca una mayor eficiencia de las operaciones. Por ello, el incremento del nivel de automatización en distintas funcionalidades de las aeronaves permitirá:

- Aumentar el nivel de seguridad de las operaciones aéreas
- Incrementar la eficiencia de las misiones

Todo ello es fundamental para el crecimiento del sector UAS en los próximos años.

A continuación, se analizan los siguientes aspectos fundamentales:

- Breve revisión del estado de las tecnologías que permitan un mayor nivel de automatización.
- Revisión de la normativa actual y futuras necesidades.
- Impacto que este tipo de tecnologías puede tener en el sector.
- Aspectos a tener en cuenta para aumentar la aceptación social.

Estado del arte

A continuación, se muestra un estado del arte de distintas tecnologías que incrementan la automatización de las operaciones con UAS (tanto para aumentar la seguridad de las operaciones, como para incrementar la eficiencia de las misiones).

Detección y evitación (DAA)

En los últimos años, gracias al avance en algoritmos de Aprendizaje Automático e Inteligencia Artificial, han surgido sistemas DAA capaces de detectar y reconocer automáticamente aeronaves no colaborativas, incluso identificando modelos específicos. Además, el aumento de la capacidad computacional a bordo permite calcular en tiempo real trayectorias factibles que permiten evitar los obstáculos detectados [1]. Ejemplos notables de sistemas DAA industriales son los sistemas Casia de Iris Automation [2] o la tecnología PilotEye de Daedalean AI [3]. Aun así, estos sistemas presentan un rango limitado y no se encuentran aún cualificados para su uso en la categoría certificada.

Por otra parte, y en relación con la detección de obstáculos cerca de la aeronave, se han logrado implementaciones exitosas en UAVs comerciales, como los de Skydio [4], donde la integración del DAA con el controlador de vuelo permite operaciones autónomas en entornos desafiantes como bosques o zonas afectadas por desastres naturales. Esta evolución representa un importante avance para la seguridad y la eficacia de los sistemas autónomos en diversos entornos operativos. Al igual que en los casos anteriores, el principal reto es asegurar la robustez y conseguir la cualificación de este tipo de sistemas.

[1] Zhou, X., Wen, X., Wang, Z., Gao, Y., Li, H., Wang, Q., ... & Gao, F. (2022). Swarm of micro flying robots in the wild. Science Robotics, 7(66), eabm5954.
[2] https://www.irisonboard.com/casia/
[3] Daedalean / PilotEye https://www.daedalean.ai/products/piloteye
[4] Skydio Autonomy™ | Skydio https://www.skydio.com/skydio-autonomy

Consciencia situacional

Para aumentar el nivel de automatización de las aeronaves, es necesario aumentar la consciencia situacional con la generación en tiempo real de mapas que sea capaz de gestionar zonas de grandes extensiones. Para ello es necesario clasificar una imagen o una escena tridimensional en múltiples segmentos o regiones y asignar una etiqueta semántica a cada segmento en función de su contenido.

Normalmente este tipo de funcionalidades se integran en una arquitectura de dos capas. La capa de bajo nivel es un esquema de mapeo multisensorial basado en funciones que integra mediciones de cámaras, GNSS e IMU, entre otros, y explota sus sinergias para construir mapas 3D detallados, precisos y robustos adecuados para las operaciones, en escenarios no estructurados y dinámicos. Mientras que la capa de alto nivel consta de un esquema de mapeo semántico que incluye técnicas de aprendizaje automático capaces de analizar el mapa multisensorial de bajo nivel y detectar, clasificar y mapear diferentes tipos de objetos que se pueden encontrar en los escenarios (por ejemplo, en un entorno exterior: árboles, coches, edificios entre otros). Una vez clasificados y mapeados, los objetos se tratan con características semánticas en el propio mapa 3D para así facilitar la toma de decisiones autónoma por parte del UAS.

Esta tecnología se encuentra a un nivel TRL bajo en el que la mayoría de los trabajos se han realizado en experimentos controlados o en laboratorio [5] y [6]. Por lo tanto, el reto de este

tipo de tecnologías es aumentar su madurez tecnológica (incluyendo su cualificación) y hacerla escalable a zonas de operación que incluya grandes extensiones.

[5] Bultmann, S., Quenzel, J., & Behnke, S. (2021, August). Real-time multi-modal semantic fusion on unmanned aerial vehicles. In 2021 European Conference on Mobile Robots (ECMR) (pp. 1-8). IEEE.
[6] Qi, X., Wang, W., Yuan, M., Wang, Y., Li, M., Xue, L., & Sun, Y. (2020). Building semantic grid maps for domestic robot navigation. International Journal of Advanced Robotic Systems, 17(1).

Inteligencia a bordo

En aplicaciones con un alto grado de automatización, las aeronaves ganan responsabilidad en la toma de decisiones. Con el advenimiento de nuevas aplicaciones que se alejan de la simple navegación entre puntos, como pueden ser la agricultura inteligente [7], la supervisión de zonas naturales [8] o inspecciones industriales [9], las misiones a realizar por las aeronaves contemplan un mayor número de estados posibles y tienen un carácter dinámico con dependencias del entorno y posibles eventos externos. En este contexto, la toma de decisiones e inteligencia a bordo es clave para orquestar las acciones que las aeronaves deben realizar para lograr un objetivo concreto, teniendo en cuenta su estado interno y el supuesto estado del entorno que nunca está libre de incertidumbre [10]. Técnicas habituales conocidas como AI-planning explotan el conocimiento de las posibles acciones y consecuencias (predicados) junto a un proceso lógico para proveer soluciones que garantizan la consecución de los objetivos. Este ágil proceso es fundamental en entornos dinámicos, cuando el agente debe replanificar continuamente sus acciones en situaciones impredecibles [11]. El conocimiento que el agente tiene sobre el mundo se puede modelar mediante diferentes formalismos. El lenguaje PDDL, del inglés Planning Domain Definition Language [12], es el más comúnmente usado y se basa en otros formalismos como pueden ser el STRIPS [13] y ADL [14]. Técnicas más recientes comienzan a incorporar el uso de Grandes Modelos de Lenguaje (LLM) [15] para generar las relaciones entre acciones y predicados y planificar con ello. El proceso de la generación de planes está estrechamente ligado al estado de su ejecución. En particular, la lista de acciones priorizada debe ser ejecutada correctamente de manera secuencial, teniendo en cuenta refinamientos del plan y replanificaciones ante el fracaso en la ejecución de alguna acción o cambios en las condiciones del entorno. Una forma habitual de definir, modificar, controlar la evolución y ejecutar las diferentes secuencias de acciones para un solo agente es a través del uso de Behaviour Trees (BT). Su uso a nivel robótico está establecido y trabajos recientes han comenzado a aplicarlos a sistemas aéreos [16].

Como se puede observar, la mayor parte de estos trabajos se han aplicado fundamentalmente en el marco de la investigación. Por todo ello, el principal reto de esta tecnología es aumentar su implementación en el sector industrial, incrementando su madurez tecnológica y avanzando hacia la cualificación de este tipo de tecnologías.

[7] D. C. Tsouros, S. Bibi, and P. G. Sarigiannidis, “A review on uav-based applications for precision agriculture,” Information, vol. 10, no. 11, 2019.
[8] R. Adade, A. M. Aibinu, B. Ekumah, and J. Asaana, “Unmanned aerial vehicle (uav) applications in coastal zone management—a review,” Environmental Monitoring and Assessment, vol. 193, pp. 1–12, 2021.
[9] B. Bendris and J. Cayero Becerra, “Design and experimental evaluation of an aerial solution for visual inspection of tunnel-like infrastructures,” Remote Sensing, vol. 14, no. 1, p. 195, 2022.
[10] Kiam, Jane Jean, et al. "An ai-based planning framework for HAPS in a time-varying environment." Proceedings of the International Conference on Automated Planning and Scheduling. Vol. 30. 2020.

[11] Yue, Longfei, et al. "Deep reinforcement learning for UAV intelligent mission planning." Complexity 2022 (2022).
[12] R. E. Fikes y N. J. Nilsson, «Strips: A new approach to the application of theorem proving to problem solving,» Artificial Intelligence, vol. 2, nº 3, pp. 189-208, 1971.
[13] E. P. D. Pednault, «ADL: Exploring the Middle Ground between STRIPS and the Situation Calculus» Proceedings of the First International Conference on Principles of Knowledge Representation and Reasoning, pp. 324-332, 1989.
[14] Fox, Maria, and Derek Long. "PDDL2. 1: An extension to PDDL for expressing temporal planning domains." Journal of artificial intelligence research 20 (2003): 61-124.
[15] Silver, Tom, et al. "PDDL planning with pretrained large language models." NeurIPS 2022 foundation models for decision making workshop. 2022.
[16] H. Goudarzi and A. Richards, "UAV Mission Monitoring and Sequencing," 2020 International Conference on Unmanned Aircraft Systems (ICUAS), Athens, Greece, 2020, pp. 1048-1055, doi: 10.1109/ICUAS48674.2020.9213870.

Despegue y aterrizaje de precisión

Son varios los desafíos tecnológicos a considerar con relación a los despegues y aterrizajes de precisión, pudiendo englobarse principalmente en los ámbitos de percepción/estimación y control. Los retos de percepción vienen de la necesidad de aterrizar en entornos con denegación de GNSS o con gran precisión, ya que se precisa el uso de posicionamiento basado en sensores (embarcados o externos). A este respecto, el nivel de complejidad varía en función de si se emplean pistas de aterrizaje estáticas, pistas móviles (plataformas flotantes, vehículos, etc.) o entornos de aterrizaje no estructurados (escenarios de emergencia, entornos naturales, etc.). Desde el punto de vista de control, el principal reto para el despegue y aterrizaje preciso viene de la capacidad de estimación y rechazo efectivo de perturbaciones aerodinámicas como el efecto suelo, además de los desafíos propios del aterrizaje en plataformas móviles o zonas poco estructuradas.

Actualmente se utilizan diversas tecnologías presentadas en diferentes estados de desarrollo (I+D, producto comercial, patentes, etc.) para llevar a cabo el aterrizaje preciso de drones. A continuación, se citan algunas de las tecnologías más comunes en estos momentos:

- Sistemas de Posicionamiento mediante GNS y RTK: El GNSS es fundamental para la navegación y el posicionamiento de los drones. Con sistemas de ayuda como la tecnología RTK (Real Time Kinematic) los drones pueden llegar a determinar su ubicación con muy alta precisión (milimétrica).
- Sensores de Ultrasonido y LIDAR: Estos sensores miden la distancia entre el dron y el suelo. Ayudan a evitar colisiones y aterrizar con mayor precisión.
- Cámaras y Sistemas de Visión: Las cámaras y sistemas de visión permiten que los drones detecten y reconozcan características del terreno, como pistas de aterrizaje o marcadores visuales.
- Marcadores Visuales (como AprilTags, Arucos, QR): Los marcadores visuales son patrones específicos que los drones pueden identificar visualmente. Se utilizan para aterrizar con precisión en ubicaciones específicas, ya que con la información capturada y procesada pueden identificar el destino, así como ubicarse y orientarse correctamente durante la maniobra.
- Antenas Ultra-Wideband (UWB) : Estas antenas proporcionan un posicionamiento local preciso cuando la señal GPS es débil o inexistente. Son útiles para el aterrizaje en áreas interiores o en entornos urbanos densos.
- Drone in a Box (DiaB): Este concepto de estaciones o bases permiten el aterrizaje autónomo, recarga y cambio de batería de los drones. Son especialmente útiles en operaciones de entrega y monitoreo continuo y permiten operaciones desatendidas (sin necesidad de una persona in situ para su control).

- Algoritmos de Control y Planificación: Las empresas desarrollan algoritmos personalizados para controlar el aterrizaje, teniendo en cuenta factores como el viento, la velocidad y la altitud.
- Aterrizaje guiado con cable : Existen sistemas y proyectos diseñados para guiar a los drones en la fase de aterrizaje de una forma mecánica, a través de un cable guía que facilita la toma del dron y su ubicación final.
- Plataformas auto estabilizadas : Algunas empresas que están desarrollando y comercializando soluciones orientadas a facilitar las maniobras de despegue y aterrizaje en condiciones de movimiento.
- Brazos robóticos para asistencia al aterrizaje : Se utilizan para preparar el drone durante la fase de despegue o para capturarlo en la fase final del aterrizaje, ubicándolo de forma precisa para su almacenamiento.

Actualmente los sistemas de aterrizaje de precisión comerciales están fundamentalmente basados para funcionar para entornos concretos que cuenten con ciertas características concretas y en la gran mayoría de las veces se cuenta con infraestructura en la zona de aterrizaje (balizas, marcadores visuales, etc.). Por lo tanto, el reto tecnológico se encuentra en desarrollar tecnologías que permita el aterrizaje de precisión en zonas no preparadas y que no requiera la instalación de ningún tipo de infraestructura.

Gestión tolerante de fallos / detección, identificación y reconfiguración de fallos FTC-redundancia

Es de gran importancia dotar a los UAS de equipos que permitan unas características de vuelo y unas operaciones seguras y confiables que minimicen el impacto de fallos que se puedan producir en determinados sistemas durante su funcionamiento. Previamente, se han debido identificar qué funciones contribuyen a una operatividad segura y el grado en el que una función automatizada actúa de manera independiente. Los tipos de fallos son referidos tanto a sensores, como a actuadores o estructurales.

Dentro de los sistemas de reducción de riesgos, un control tolerante de fallos (FTC, Fault-Tolerant Control) debe establecer un auto seguimiento y hacer que se mantenga el funcionamiento de manera autónoma y adecuada incluso cuando uno o más de sus componentes fallen. Como principales sistemas de gestión se encuentran:

- Técnicas de redundancia y diagnóstico de fallos; basadas principalmente en: i) redundancia de hardware, en sistemas de propulsión, sensores y comunicaciones; ii) redundancia analítica, basada en modelos o en conocimiento; y iii) procesado de la señal, las medidas de las señales contienen información que pueden identificar “síntomas” de fallos y su detección.
- El control de fallos, dividido en: i) pasivos, que no dependen de información acerca de fallos (control robusto) y suelen integrar redundancia; ii) activos, con un módulo de detección de fallos (que monitoree constantemente su estado e identifique problemas antes de que afecten al funcionamiento), aislamiento (localización exacta y que no afecte negativamente a otros componentes), así como sistemas de recuperación que puedan corregir automáticamente los errores o cambiar a un modo de operación alternativo; e iii) híbridos.

Los avances en tecnología y diseño deben continuar para garantizar la seguridad de las operaciones, mayor disponibilidad al permitir la operatividad a pesar de los fallos, menor tiempo de inactividad, mayor fiabilidad, capacidad de recuperación y menores costes de mantenimiento al reducir la intervención manual. Actualmente la mayoría de los sistemas tolerantes a fallos están basados en redundancia HW, sin embargo, eso implica un aumento de peso y dimensiones, reduciendo el tiempo de vuelo o aumentando el tamaño de la aeronave. El reto está en el desarrollo de sistemas de tolerante a fallos SW que permitan una

reconfiguración del sistema pudiendo mantener la seguridad en vuelo de la aeronave maximizando las complementariedades existentes entre sensores y actuadores.

Ciberseguridad

A medida que aumenta el número de drones y su conectividad con redes externas, también crece el riesgo de ciberataques a los UAS, lo que ha hecho crecer el interés para garantizar la privacidad, la integridad y la disponibilidad de los datos, así como para proteger a los usuarios y las operaciones. En este sentido, las soluciones de ciberseguridad para UAS son cada vez más sofisticadas y deben evolucionar constantemente para abordar los nuevos riesgos y amenazas emergentes. Aunque es un tema relativamente nuevo, pues ha surgido a medida que el uso de drones se ha vuelto más extendido, ya existen algunos antecedentes relevantes en el ámbito de la ciberseguridad para drones, por ejemplo:

- En 2013, un grupo de investigadores de seguridad descubrieron una vulnerabilidad en el protocolo de comunicación de drones militares Predator y Reaper. Esta vulnerabilidad permitía que un atacante interceptara las señales de control del dron y tomara el control del mismo.
- En 2019, el Departamento de Seguridad Nacional de EE. UU. emitió una alerta de seguridad que advertía sobre el riesgo de que los drones fabricados en China pudieran ser utilizados para espiar a los ciudadanos estadounidenses y recopilar datos sensibles. La alerta también señalaba que los drones podían ser vulnerables a ataques cibernéticos.

Por otro lado, los UAS poseen diferentes sistemas HW y SW (vehículo, autopiloto, propulsión, energía, posicionamiento, carga de pago, estación de control, comunicaciones, sistemas de back-end para almacenamiento, procesado y comunicación con otros sistemas), que no están exentos de vulnerabilidades y consecuentes riesgos, intencionados o no. Algunos ejemplos de VULNERABILIDADES en términos de ciberseguridad son:

1. En el software: puede ser explotado por atacantes para tomar el control del dron.
2. En la comunicación o el protocolo de control: si los datos de control y telemetría se transmiten sin cifrado o fácilmente interceptables, el dron podría ejecutar maniobras peligrosas o modificarse la misión
3. Físicas: manipulación física, como la eliminación de componentes, la modificación de hardware o la inyección de señales para interferir con la comunicación inalámbrica.
4. En la gestión de acceso: Si los drones están conectados a una red o a otros sistemas, pueden ser vulnerables a los mismos ataques que otros dispositivos conectados, como el phishing o la fuerza bruta para adivinar contraseñas.

Por lo tanto, resulta patente la necesidad y especial interés de establecer y llevar a la práctica metodologías y herramientas que pongan a prueba los drones en diferentes escenarios, condiciones y operaciones, con el fin de evaluar los límites técnicos y operativos, así como identificar y clasificar en la medida de lo posible los riesgos y vulnerabilidades que puedan afectar a los sistemas. Cuanto mayor sea la información obtenida de antemano en ensayos de ciberseguridad, más recursos tendrán los usuarios finales para la protección y actuación ante una situación de amenaza.

Obviamente la ciberseguridad de cualquier vehículo conectado es un aspecto de suma importancia hoy en día, pero resulta de especial interés en vehículos que tengan una mayor autonomía en su operación. Especialmente en UAS altamente autónomos es un aspecto poco investigado y que cobrará una gran importancia en los próximos años. Por último, cabe señalar que ya existe un cuerpo regulatorio para prevenir estos riesgos, aunque cabe dudar si resultará suficiente ante posibles ataques[1].

[1] Para una exposición de la normativa vigente (Estrategia de Ciberseguridad de la OACI, la legislación

Swarming

Swarming se refiere a un comportamiento coordinado exhibido por un grupo de vehículos aéreos no tripulados en el que varios UAS trabajan juntos de manera colaborativa para lograr un objetivo común. En un enjambre, los UAV individuales se comunican entre sí y exhiben un comportamiento colectivo. Este comportamiento colectivo permite a los UAV realizar tareas como inspección cooperativa, seguimiento cooperativo, vigilancia y reconocimiento, entre otras. Hay dos enfoques principales para controlar un enjambre: centralizado, donde toda la información se envía a un punto común, que puede ser una estación terrestre o una plataforma líder en el enjambre, que procesa los datos y controla todos los UAS; y descentralizado, donde cada UAS toma sus propias decisiones a bordo en función de la información que recibe de las otras plataformas del enjambre y de sus propios sensores. Los principales desafíos a resolver dentro de esta tecnología son la comunicación dentro del enjambre, la planificación de rutas libre de colisiones, la asignación de tareas, la toma de decisiones, la interoperabilidad y la estandarización. Además del enjambre de vehículos aéreos no tripulados, estas tecnologías también se pueden aplicar a enjambres multidominio donde los vehículos aéreos se combinan con vehículos marítimos o terrestres para diferentes operaciones.

Hay numerosos ejemplos en el sector civil de proyectos de enjambre. Como, por ejemplo, el proyecto europeo ASSISTANCE, donde se diseñó un enjambre para ayudar en catástrofes desplegando una red de comunicación utilizando UAV como repetidor. También cabe mencionar el proyecto AERIAL-CORE donde se ha demostrado la capacidad de realizar una inspección de líneas eléctricas con un equipo de varios UAS colaborativos. En el ámbito militar, Airbus está desarrollando conceptos de Manned-Unmanned Teaming (MUT) donde un único operador es capaz de dirigir un equipo de UAS únicamente a partir de acciones de alto nivel. Sin embargo, como se puede ver en los proyectos mencionados, este tipo de tecnología aún solo se ha validado en TRL5-6 y todavía falta aumentar su madurez tecnológica (incluyendo la cualificación) para integrarlos en productos comerciales.

de la UE y nacional sobre ciberseguridad en el ámbito de la aviación, UAS y U-Space, puede consultarse en “Bustos Moreno, Y.: "The Implementation of U-space: Open Challenges from the Legal-Private Perspective", Pastor Sempere, C. (Ed.). *Governance and Control of Data and Digital Economy in the European Single Market. Legal Framework for New Digital Assets, Identities and Data Space*. Law, Governance and Technology Series Springer, 2025, pp. 489-515.

Estado actual de la regulación y futuras necesidades

Pese a que a corto plazo no se prevé la implantación de vehículos aéreos autónomos, la normativa directamente aplicable a los UAS ya se ha adaptado a los mismos, aunque solo se trata de una modificación formal de momento. El marco comunitario aplicable *ad hoc* a los UAS, como nuestra legislación interna, ya ha incorporado en sus respectivos ámbitos de aplicación el concepto de *aeronaves autónomas*, de momento, según parece como operaciones *autorizables* (art. 11 Ley 48/1960, de 21 de julio, sobre Navegación Aérea, en adelante, LNA, a través del RD-L 26/2020, de 7 de julio, art. 3.30 Reglamento 2018/1139 (en adelante Reglamento UE Base) y art. 2.1 Reglamento de Ejecución (UE) 2019/947), conceptos sobre los que se basa el Real Decreto 517/2024, como recoge en la Exposición de Motivos y su Anexo II[2])
La regulación europea permite a día de hoy la operación de sistemas aéreos autónomos en la categoría específica (Reglamento 945 y 947). Sin embargo, aún no se ha desarrollado material guía o medios de cumplimiento que defina los requisitos que deben cumplir las funcionalidades automatizadas para ser incluidas en una autorización operacional. En este aspecto es relevante mencionar el documento "JARUS Methodology for Evaluation of Automation for UAS Operations" publicado en abril de 2023 y desarrollado por la asociación JARUS (asociación de expertos de las Autoridades de Aviación Nacionales de 67 países y que cuenta con 69 miembros, incluyendo AESA, EASA y EUROCONTROL).

En este documento propone un esquema de clasificación y análisis de impacto que pueden dar soporte en el análisis del riesgo de las operaciones automatizadas de UAS haciendo uso de la metodología SORA (también desarrollada por JARUS y aceptada por EASA como una metodología válida para el análisis de riesgo en la categoría específica. También introduce el concepto de Dominio de Diseño Operativo (ODD) como un mecanismo para abarcar funciones automatizadas para ayudar a gestionar un entorno operativo multidimensional complejo. Esto permite una evaluación funcional de la automatización en lo que se refiere a las interacciones hombre-máquina, reconociendo que, en una operación particular, diferentes funciones de la aeronave pueden automatizarse en diferentes niveles. En el *Nivel 5,* los humanos quedarían fuera del circuito. El sistema autónomo no recibiría ayuda de personas para realizar ninguna función[3].
Por otra parte y como se ha comentado en la sección anterior, uno de los aspectos claves para incrementar la madurez tecnológica de las tecnologías de automatización es la cualificación/certificación de este tipo de sistemas. En este aspecto, la irrupción de la Inteligencia Artificial en muchas de las tecnologías de automatización complica este aspecto, sobre todo para sistemas críticos de vuelo en operaciones de alto riesgo que requieran niveles de aseguramiento altos (IDAL A o B). Aunque EASA está llevando a cabo un esfuerzo importante en trabajar en cómo cualificar este tipo de tecnologías, y ha publicado en marzo de 2024 la segunda versión del "Concept Paper"[4] sobre IA y Aprendizaje automático (Machine Learning o ML), todavía se ha

[2] En el derogado Real Decreto 1036/2020, expresamente, se informaba que no estaba permito el vuelo de las aeronaves autónomas. En concreto, determinaba que: "Este real decreto, en coherencia con la convención internacional en la materia y las normas de derecho comparado no regula el uso de aeronaves civiles no tripuladas que no permiten la intervención del piloto en la gestión del vuelo, las denominadas aeronaves autónomas, cuyo uso en el espacio aéreo español y en el que España es responsable de la prestación de servicios de tránsito aéreo no está permitido. Por su parte, el art. 4 del mismo Real Decreto, declaraba, con relación a los requisitos generales de uso de las aeronaves pilotadas por control remoto (RPA), que el uso de aeronaves pilotadas por control remoto (RPA) requerirá, en todo caso que su diseño y características *permitan al piloto intervenir en el control del vuelo, en todo momento.* El piloto remoto será, en todo momento, el responsable de detectar y evitar posibles colisiones y otros peligros".
[3] Se declara en dicho documento que, respecto a la forma de evitar una colisión en pleno vuelo, la función que opera en L5 no tendría interacción en tiempo real entre un piloto y la maniobra de evitación. Cualquier evento o problema podría ser revisado / analizado después del vuelo.
[4] https://www.easa.europa.eu/en/downloads/139504/en

limitado la posible cualificación a niveles IDAL C o D y a niveles de automatización bajos (AI level 1A, 1B y 2A). Por lo tanto, actualmente los sistemas que implementen funcionalidades automatizadas basadas en IA y ML deberían centrarse en asistencia al piloto/operador o como mucho en funcionalidades que requieran la colaboración entre ambos y no requerir un nivel de aseguramiento en el desarrollo mayor de IDAL C. Para mayores niveles de automatización o de aseguramiento, todavía hace falta avanzar en la regulación y material guía.

Por su parte el Reglamento (UE) 2024/1689, en adelante Reglamento (UE) IA, que recientemente ha entrado en vigor (aunque de forma escalada irá resultando aplicable)[5] va a suponer un hándicap de cumplimiento en esta materia, en la medida que conforme se elevan los niveles de automatización, se van a emplear distintos sistemas de IA, algunos de ellos aplicables a las aeronaves y gestión del tráfico aéreo[6]. Los sistemas de IA pueden utilizarse de manera independiente o como componentes de un producto, citándose como ejemplo la aviación, con independencia de si el sistema forma parte físicamente del producto (integrado) o contribuye a la funcionalidad del producto sin formar parte de él (no integrado), Considerando (12).

Sin embargo, no se aborda directamente la inclusión de los vehículos autónomos (*full* en su consideración integral), sino que el Reglamento (UE) IA se ocupa la integración de sistemas de IA como componentes de producto, exigiéndose la necesidad de supervisión humana. En base a ello, podría dudarse si los vehículos autónomos entrarían en su ámbito de aplicación, pues como dispone el art. 14 Reglamento (UE) IA: "1. Los sistemas de IA de alto riesgo se diseñarán y desarrollarán de modo que puedan ser vigilados de manera efectiva por personas físicas durante el período que estén en uso, lo que incluye dotarlos de herramientas de interfaz humano-máquina adecuadas". A su vez, el inciso 3º del art. 14 declara que: "Las medidas de supervisión serán proporcionales a los riesgos, al nivel de autonomía y al contexto de uso del sistema de IA de alto riesgo" y, en el apartado 4º, que: "las personas físicas a quienes se encomiende la supervisión humana puedan, según proceda y de manera proporcionada: d) decidir, en cualquier situación concreta, no utilizar el sistema de IA de alto riesgo o descartar, invalidar o revertir los resultados de salida que este genere"; así como "e) intervenir en el funcionamiento del sistema de IA de alto riesgo o interrumpir el sistema pulsando un botón de parada o mediante un procedimiento similar que permita que el sistema se detenga de forma segura"[7]. Por lo que puede deducirse que no se podría permitir al día de hoy el nivel 5 de automatización, conforme a la clasificación de JARUS. No obstante, hasta que la Comisión europea no dicte actos delegados o de ejecución en desarrollo del Reglamento (UE) IA, no se conocerá con certeza los aspectos a modificar o el articulado aplicable cuando se emplee tecnología de IA.

Otra cuestión pendiente de resolver es la aplicación coordinada entre los distintos cuerpos legales:

[5] Reglamento (UE) 2024/1689 del Parlamento europeo y del Consejo de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial), también denominada "Ley de Inteligencia Artificial", a la que en adelante nos referiremos como AIA (atendiendo a sus siglas en inglés), fue publicada en el DOUE, con entrada en vigor el 1 de agosto de 2024. En el art. 113 Reglamento IA se establecen distintas fechas de aplicación para sus disposiciones.

[6] Como se indica en el Considerando 12 Reglamento (UE) IA, los sistemas de IA están diseñados para funcionar con distintos niveles de autonomía, lo que significa que pueden actuar con cierto grado de independencia con respecto a la actuación humana y tienen ciertas capacidades para funcionar sin intervención humana. La capacidad de adaptación que un sistema de IA podría mostrar tras su despliegue se refiere a las capacidades de autoaprendizaje que permiten al sistema cambiar mientras está en uso.

[7] Art. 9 Reglamento (UE) IA: Modificaciones del anexo III: "Cuando evalúe la condición prevista en el apartado 1, letra b), la Comisión tendrá en cuenta los criterios siguientes: d) el grado de autonomía con el que actúa el sistema de IA y la posibilidad de que un ser humano anule una decisión o recomendaciones que puedan dar lugar a un perjuicio". Y el art. 26 (2) 2. dispone que: "Los responsables del despliegue encomendarán la supervisión humana a personas físicas que tengan la competencia, la formación y la autoridad necesarias".

el marco comunitario sobre aviación y UAS, con relación al Reglamento (UE) IA y sus normas de desarrollo[8]. Al efecto, el Anexo I del Reglamento IA nombra entre la lista de *actos legislativos de armonización* de la Unión al Reglamento Base[9], "en la medida en que afecte al diseño, la producción y la introducción en el mercado de aeronaves a que se refiere el artículo 2, apartado 1, letras a) y b), por lo que respecta a las aeronaves no tripuladas y sus motores, hélices, componentes y equipos para controlarlas a distancia".

Con relación a la integración de sistemas de IA dentro de UAS o aeronaves en general, así como en sistemas de gestión del tráfico aéreo (ej. U-Space), encontramos varias referencias aeronáuticas en el articulado del Reglamento (UE) 2024 de gran calado, con relación a su consideración como "sistemas de IA de alto riesgo"[10] como el art. 108 que modifica el Reglamento Base. No se trata de un tema baladí a la vista de las exhaustivas obligaciones previstas en el Reglamento (UE) 2024 con relación a los "sistemas de alto riesgo" y que, sin duda, podrían suponer un efecto disuasorio para la inversión europea en esta industria, aumentando así la brecha de competitividad con relación a Estados Unidos (véase el reciente Informe Dragui[11]), si bien existe todavía un margen para su exigencia, dado que no resultarán aplicables hasta dentro de tres años, en concreto, a partir del 2 de agosto de 2027[12]. Por otro lado se observa que el criterio empleado para delimitar el riesgo en el marco legislativo comunitario vigente sobre UAS (categorías operacionales[13] y certificaciones) no coincide con el previsto en el Reglamento (UE) IA. Es por ello la importante labor futura de coordinación y armonización entre este cuerpo legal (básicamente

[8] Sobre esta problemática, se sigue a Bustos Moreno, Y. "Aplicaciones de la inteligencia artificial conforme a la Ley de Movilidad Sostenible. Consideraciones en torno al régimen de responsabilidad civil acorde con la innovación", Inteligencia Artificial y Derecho de Daños. Cuestiones Actuales acorde al Reglamento (UE) 2024/1689, Dykinson, 2024, pp. 119-148.

[9] Reglamento (UE) 2018/1139 del Parlamento Europeo y del Consejo, de 4 de julio de 2018, sobre normas comunes en el ámbito de la aviación civil y por el que se crea una Agencia de la Unión Europea para la Seguridad Aérea y por el que se modifican los Reglamentos (CE) n.o 2111/2005, (CE) n.o 1008/2008, (UE) n.o 996/2010 y (UE) n.o 376/2014 y las Directivas 2014/30/UE y 2014/53/UE del Parlamento Europeo y del Consejo y se derogan los Reglamentos (CE) n.o 552/2004 y (CE) n.o 216/2008 del Parlamento Europeo y del Consejo y el Reglamento (CEE) n.o 3922/91 del Consejo

[10] *Artículo 6* Reglas de clasificación de los sistemas de IA de alto riesgo
1.Con independencia de si se ha introducido en el mercado o se ha puesto en servicio sin estar integrado en los productos que se mencionan en las letras a) y b), un sistema de IA se considerará de alto riesgo cuando reúna las dos condiciones que se indican a continuación: a)que el sistema de IA esté destinado a ser utilizado como componente de seguridad de un producto que entre en el ámbito de aplicación de los actos legislativos de armonización de la Unión enumerados en el anexo I, o que el propio sistema de IA sea uno de dichos productos, y b) que el producto del que el sistema de IA sea componente de seguridad con arreglo a la letra a), o el propio sistema de IA como producto, deba someterse a una evaluación de la conformidad de terceros para su introducción en el mercado o puesta en servicio con arreglo a los actos legislativos de armonización de la Unión enumerados en el anexo I. 2.Además de los sistemas de IA de alto riesgo a que se refiere el apartado 1, también se considerarán de alto riesgo los sistemas de IA contemplados en el anexo III. 3.No obstante lo dispuesto en el apartado 2, un sistema de IA a que se refiere el anexo III no se considerará de alto riesgo cuando no plantee un riesgo importante de causar un perjuicio a la salud, la seguridad o los derechos fundamentales de las personas físicas, también al no influir sustancialmente en el resultado de la toma de decisiones".

[11] Informe *Dragui* "The future of European competitiveness", disponible en https://commission.europa.eu/topics/strengthening-european-competitiveness/eu-competitiveness-looking-ahead_en.

[12] El art. 113 AIA dispone que el artículo 6, apartado 1, y las obligaciones correspondientes del presente Reglamento serán aplicables a partir del 2 de agosto de 2027.

[13] Artículo 2 RD 517/2024: "Definiciones. 1. A los efectos de este real decreto, además de la definición de «Actividades o servicios no EASA», se entenderá por: a) Categoría «abierta»: la categoría de operaciones de UAS establecida en los artículos 3.a) y 4 del Reglamento de Ejecución; b) Categoría «específica»: la categoría de operaciones de UAS establecida en los artículos 3.b) y 5 del Reglamento de Ejecución; c) Categoría «certificada»: la categoría de operaciones de UAS establecida en los artículos 3.c) y 6 del Reglamento de Ejecución;

el Reglamento (UE) IA, pero también la Directiva de Responsabilidad por Productos Defectuosos[14] y la Propuesta de Directiva sobre responsabilidad en materia de IA (en adelante, PDRCIA)[15], que de momento ha sido retirada por la Comisión Europea.

Comenzando por referirnos al Reglamento (UE) IA, en primer término, cabe constatar que bajo dicha clasificación se incluyen, entre otros, los componentes de seguridad de productos o sistemas, o que son en sí mismos productos o sistemas que entran en el ámbito de aplicación del Reglamento (CE) n. 300/2008 del Parlamento Europeo y del Consejo, de 11 de marzo de 2008, sobre normas comunes para la seguridad de la aviación civil y por el que se deroga el Reglamento (CE) n. 2320/2002 *procede modificar dichos actos* para garantizar que, cuando la Comisión adopte actos delegados o de ejecución pertinentes basados en ellos, *tenga en cuenta los requisitos obligatorios para los sistemas de IA de alto riesgo* previstos en el presente Reglamento, atendiendo a las *particularidades técnicas y reglamentarias de los distintos sectores y sin interferir* con los mecanismos y las autoridades de gobernanza, evaluación de la conformidad y control del cumplimiento vigentes establecidos en dichos actos (Considerando 49) y, con mención expresa a la aviación, encontramos el Considerando 50 y especialmente la obligación de modificación del Reglamento Base, en virtud del art. 108 del Reglamento (UE) IA. De forma similar, el art. 2.3. de la EU *Cyber Resilience Act*[16], tampoco se aplica los productos, componentes y equipos aeronáuticos, incluidos los programas informáticos con elementos digitales que hayan sido certificados de conformidad con el Reglamento (UE) 2018/1139[17].

En segundo término, se consideran "sistemas de alto riesgo" los sistemas de IA destinados a ser utilizados como componentes de seguridad en la gestión y explotación *de infraestructuras digitales críticas* (véase art. 6.2, Anexo III y Considerando 55 del Reglamento (UE) IA). Queda por determinar si U-Space puede considerarse una «infraestructura digital crítica» y si el funcionamiento de alguno de los servicios de U-Space encaja dentro de los sistemas de IA destinados a ser utilizados como componentes de seguridad en su gestión y funcionamiento[18]. La respuesta se encuentra en la Directiva CER[19], a la que remite el Reglamento sobre la IA

[14] Esta Directiva ha sido aprobada el 12 de marzo de 2024 y está pendiente de publicación en el DOUE.

[15] Propuesta de DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial (Directiva sobre responsabilidad en materia de IA), COM/2022/496 final, 28 de septiembre de 2022.

[16] El Reglamento de Ciberresiliencia, de 23 de octubre de 2024, relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales y por el que se modifica el Reglamento (UE) n.º 168/2013 y el Reglamento (UE) 2019/1020 y la Directiva (UE) 2020/1828 se aplicará a todos los productos conectados directa o indirectamente a otro dispositivo o a una red. Se introducen algunas excepciones en el caso de los productos para los que ya se establecen requisitos de ciberseguridad en otras normas vigentes de la UE, por ejemplo, los productos sanitarios y aeronáuticos y los automóviles. Respecto a esta exclusión, véase la explicación aportada en el Considerando 27.

[17] Con relación al Reglamento IA, la EU *Cyberresilience Act* dispone que los productos con elementos digitales considerados sistemas de inteligencia artificial (IA) de alto riesgo en virtud del artículo 6 del Reglamento (UE) 2024/1689 del Parlamento Europeo y el Consejo21 que entren en el ámbito de aplicación del presente Reglamento deben cumplir los requisitos esenciales de ciberseguridad establecidos en el presente Reglamento. Cuando estos sistemas de IA de alto riesgo cumplan los requisitos esenciales de ciberseguridad establecidos en el presente Reglamento, debe considerarse que cumplen los requisitos de ciberseguridad establecidos en el artículo 15 del Reglamento (UE) 2024/1689 en la medida en que dichos requisitos estén contemplados en la declaración UE de conformidad expedida en virtud del presente Reglamento o en partes de esta (Considerando 51).

[18] Sobre el razonamiento expuesto en el texto, seguimos a Bustos Moreno, Y.: "The Implementation of U-space: Open Challenges from the Legal-Private Perspective", Pastor Sempere, C. (Ed.). *Governance and Control of Data and Digital Economy in the European Single Market. Legal Framework for New Digital Assets, Identities and Data Space.* Law, Governance and Technology Series Springer, 2025, pp. 489-515.

[19] Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo, que deroga la Directiva 2008/114/CE del Consejo y establece la nueva Directiva sobre la capacidad de recuperación de las entidades críticas,

(considerando 55). La integración de U-Space bajo el paraguas del Reglamento (UE) IA y de la Directiva CER parece afirmativa, aunque no se indique expresamente. Podemos deducirlo al referirse a las infraestructuras críticas digitales, las compañías aéreas, los aeropuertos y las entidades gestoras de aeropuertos (Anexo[20] y art. 6 de la Directiva CER[21]. Esta conclusión también se extrae de la definición de «entidad crítica», e «infraestructura crítica que aporta el art. 2.1 y 4, respectivamente Directiva CER[22].

Con la entrada en vigor del Reglamento de Ejecución (UE) 2021/664 de la Comisión Europea el 22 de abril de 2021[23], se establece en la Unión Europea un marco regulatorio específico para el U-Space, o espacio aéreo designado para la operación de drones. Esta regulación busca responder al crecimiento y desarrollo de la aviación no tripulada, integrándola de manera segura y estructurada dentro del sistema de aviación europeo, en armonía con la aviación tripulada. Así, el U-Space se configura como una pieza clave dentro del Cielo Único Europeo y una herramienta para el despliegue seguro y coordinado de la aviación no tripulada en el espacio aéreo común.
El concepto de "espacio aéreo U-Space" se refiere a áreas geográficas específicas definidas por cada Estado miembro de la UE, en las cuales las operaciones con drones serán gestionadas mediante servicios de U-Space. Dichos servicios, basados en la automatización y digitalización de las funciones de gestión, permiten un acceso seguro y eficiente al espacio aéreo. El reglamento establece los criterios técnicos y operacionales que los proveedores de servicios U-Space deben cumplir para garantizar la seguridad y eficiencia de las operaciones.

Este espacio está diseñado para facilitar la coexistencia de la aviación tripulada y no tripulada en el mismo entorno, estableciendo los principios que deben seguir las autoridades nacionales para la designación, gestión y supervisión de estas zonas. Además, se incorpora un esquema de responsabilidades compartidas que abarca a los Estados miembros, autoridades de aviación y proveedores de servicios, garantizando que el espacio aéreo U-Space funcione conforme a los estándares de seguridad y eficiencia definidos a nivel europeo.

La Estrategia de Drones 2.0 de la Comisión Europea [24]subraya que el U-Space no solo es un marco de seguridad, sino también un incentivo regulador para el desarrollo económico. Al regular el

promulgada el 14 de diciembre de 2022. Los Estados miembros tienen hasta el 17 de octubre de 2024 para transponer los requisitos de la Directiva CER a la legislación nacional (en lo sucesivo, «Directiva CER»).

[20] En el Anexo de la Directiva CER se determina expresamente que son entidades críticas las compañías aéreas, tal como se definen en el artículo 3, punto 4, del Reglamento (CE) n.º 300/2008 utilizadas con fines comerciales; las entidades gestoras de aeropuertos, tal como se definen en el artículo 2, punto 2, de la Directiva 2009/12/CE del Parlamento Europeo y del Consejo; los aeropuertos, tal como se definen en el artículo 2, punto 1, de dicha Directiva, incluidos los aeropuertos de la red principal enumerados en la sección 2 del anexo II del Reglamento (UE) n.º 1315/2013 del Parlamento Europeo y del Consejo, y las entidades que exploten instalaciones auxiliares dentro de las instalaciones aeroportuarias definidas en la sección 2 del anexo II del Reglamento (UE) n. 1315/2013 del Parlamento Europeo y del Consejo y las entidades que exploten instalaciones auxiliares en los recintos de los aeropuertos.

[21] El art. 6 establece además que, en relación con la identificación de las entidades críticas, «a más tardar el 17 de julio de 2026, los Estados miembros identificarán las entidades críticas para los sectores y subsectores enumerados en el anexo".

[22] Art. 2.1. Directiva CER: «entidad crítica»: «una entidad pública o privada identificada por un Estado miembro de conformidad con el art. 6 como perteneciente a una de las categorías que figuran en la tercera columna del cuadro del anexo». Art. 2(4) Directiva CER: «infraestructura crítica»: «un elemento, instalación, equipo, red o sistema, o parte de un elemento, instalación, equipo, red o sistema, que sea necesario para la prestación de un servicio esencial». Art. 2. 5) «servicio esencial»: un servicio crucial para el mantenimiento de las funciones vitales de la sociedad, las actividades económicas, la salud y la seguridad públicas o el medio ambiente».

[23]Reglamento de Ejecución (UE) 2021/664 de la Comisión Europea el 22 de abril de 2021 https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32021R0664&from=EN

[24] Iniciativa Comisión Europea Estrategia 2.0 para los drones. Movilidad sostenible en Europa. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13046-Una-Estrategia-20-para-los-drones-a-fin-de-fomentar-una-movilidad-sostenible-e-inteligente-en-Europa_es

acceso y la gestión del espacio aéreo, la UE facilita la creación de nuevos modelos de negocio en sectores donde el uso intensivo de drones genera beneficios, tales como la agricultura, construcción, vigilancia, sanidad, seguridad pública y emergencias.

Como se ha analizado anteriormente, con la entrada en vigor del Reglamento de Ejecución (UE) 2021/664 de la Comisión Europea, se sientan las bases para la integración de la aviación no tripulada en el sistema de aviación europeo mediante la creación del espacio aéreo U-Space. Este marco regula el uso de drones en áreas específicas, con el objetivo de gestionar de forma segura el tránsito de estas aeronaves y de permitir su convivencia con la aviación tripulada. En este contexto, surgen nuevos desafíos regulatorios y jurídicos que afectan de manera directa e indirecta los Derechos Fundamentales reconocidos en el Título I de la Constitución Española.
La creciente implementación de drones en el ámbito civil plantea interrogantes sobre el impacto de estos dispositivos en derechos fundamentales[25] garantizados constitucionalmente en España, tales como el derecho a la intimidad personal y familiar (artículo 18 CE), el derecho a la libertad y seguridad (artículo 17 CE) y la protección de datos personales. El análisis de estos impactos es esencial para entender cómo la normativa del U-Space debe ajustarse no solo a los requisitos técnicos de operación, sino también a los límites constitucionales que protegen a los ciudadanos de posibles abusos en el uso de esta tecnología. La regulación del U-Space en la UE y su aplicación en los Estados miembros debe operar con una cautela minuciosa para evitar posibles conflictos con los derechos fundamentales. En este sentido, la normativa de drones en el contexto del U-Space debe alinearse con los derechos constitucionales recogidos en el ordenamiento jurídico español.

Queda por último referirnos a la necesidad de aplicación coordinada en materia de responsabilidad civil. La regulación del régimen de aplicación ante la irrogación de posibles daños a terceros, es decir, la responsabilidad civil, es otro de los puntos críticos y que, al día de hoy, continúa sin soluciones armonizadas en la UE y, en el caso de España, con profundas deficiencias en nuestra regulación *ad hoc*[26]. El Reglamento (UE) IA poco establece al respecto[27], salvo en materia de daños infligidos como resultado de la experimentación realizada en el espacio controlado de pruebas para remitir al Derecho de la Unión y nacional en materia de responsabilidad y disponer una exención de multas (art. 57.12), así como en el caso de pruebas de sistemas de IA de alto riesgo en condiciones reales fuera de los espacios controlados de pruebas para la IA, donde también se habilita la misma delegación (art. 60.9).

Por otro lado, y en relación a la responsabilidad civil de la operación de sistemas aéreos autónomos, se constata que la PDRCIA evita entrar a regular el régimen sustantivo de responsabilidad civil de sistemas de IA de alto riesgo y expresamente declara que no va a afectar a "las normas del Derecho de la Unión que regulan las condiciones de responsabilidad en el ámbito del transporte" en el caso de demandas de responsabilidad civil extracontractual subjetiva (basada en la culpa) por daños y perjuicios, sin aportar más regulación que determinados expedientes para

[25] La afección de los drones a los derechos fundamentales. Efrén Díaz Díaz. https://www.derechogeoespacial.com/la-afeccion-de-los-drones-a-los-derechos-fundamentales/

[26] No se aborda en este White Paper la necesidad de adaptación de la regulación sobre responsabilidad contractual de las aeronaves altamente automatizadas o autónomas, en el caso del transporte de mercancías o personas. Recientemente, la OACI ha actualizado los límites indemnizatorios viajes aéreos internacionales, información disponible en: https://www.icao.int/Newsroom/Pages/ES/International-air-travel-liability-limits-set-to-increase,-enhancing-customer-compensation--.aspx#:~:text=%E2%80%8BMontr%C3%A9al%2C%2018%20October%202024,will%20increase%20on%2028%20December

[27] Únicamente el art. 86 Reglamento (UE) IA se destina a establecer el derecho de explicación de toda persona que se vea afectada por una decisión que se adopte basándose en los resultados de calidad de un sistema de IA de alto riesgo, entre los que se excluyen precisamente los utilizados como componentes de seguridad en la gestión y explotación de infraestructuras digitales críticas, el tráfico por carretera y suministros esenciales (Anexo III punto 2), Reglamento (UE) IA.

facilitar la carga de la prueba, como presunciones de causalidad (arts. 1, 3 y 4 principalmente). Se olvida de que se suele partir de un régimen sin culpa o de responsabilidad objetiva en las actividades típicamente por riesgo, como se ha venido calificando la navegación aérea, donde no se tiene en cuenta el deber de diligencia para responsabilizar al operador[28].

Efectivamente, en España, en caso de irrogarse daños a terceros en el ámbito de la navegación aérea, se aplica como primer estadio un régimen de responsabilidad estricta, con límites indemnizatorios que no están adaptados ni a las aeronaves no tripuladas y, mucho menos, a las altamente automatizadas y posiblemente autónomas, conforme dispone la anticuada LNA (y normativa de desarrollo reglamentario), a pesar de contemplarse en el art. 11 LNA las operaciones autónomas, como hemos señalado. Además, la obligación de aseguramiento se ha eximido para ciertas categorías, pese a la importante garantía indemnizatoria que supone en estos casos de responsabilidad civil, según ha dispuesto el art. 8 del Real Decreto 517/2024. No parece la mejor medida, con visión a largo plazo, en caso de que los operadores tuviesen que atender a responsabilidades civiles de cierta entidad económica. Además, si se llegase a demostrar la falta de diligencia, en caso de irrogarse daños por encima de los topes indemnizatorios, habría que indemnizar *in integrum* a las víctimas[29].

[28] El demandante debe demostrar la culpa del demandado con arreglo a las normas nacionales o de la Unión aplicables. Esta culpa puede determinarse, por ejemplo, por incumplimiento de un deber de diligencia en virtud de la Ley de IA o de otras normas establecidas a escala de la Unión, como las que regulan el uso de la supervisión y la toma de decisiones automatizadas para el trabajo en plataformas o las que regulan el funcionamiento de aeronaves no tripuladas, ap. 4 PDRCIA. Sin embargo, recientemente se ha propuesto dar entrada explícita a aplicaciones de IA, adicionales a las ya contempladas como de "alto riesgo", vinculadas con los vehículos autónomos (o la IA relacionada con el transporte), proponiendo la sustitución de "alto riesgo" por "alto impacto" en atención al riesgo individual que pueden suponer para un pequeño grupo de personas, el impacto de estos vehículos aéreos, PARLAMENTO EUROPEO: *Complementary impact assessment. Proposal for a directive on adapting non-contractual civil liability rules to artificial intelligence*, Philip Hacker STUDY EPRS | Research Service Ex-Ante Impact Assessment Unit PE 762.861– September 2024. No se trata de una proposición nueva, sino que ya la Propuesta de Reglamento contenida en la Resolución del Parlamento Europeo de 20 de octubre de 2020 con «Recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial» sí calificaba, erróneamente pues no todos los UAS pueden calificarse de "alto riesgo", los siguientes sistemas de IA: 1) aeronaves no tripuladas (UAS) según el artículo 3, punto 30, del Reglamento (UE) 2018/1139, es decir, drones que operan o están diseñados para operar de forma autónoma o bajo control remoto sin piloto a bordo (en el sector del transporte); 2) vehículos con niveles de automatización 4 y 5, de acuerdo con la norma SAE J3016 (en el sector del transporte);

[29] Ampliamente, sobre esta problemática, puede consultarse Bustos Moreno, Y.: "**La irrupción de los drones (sistemas de aeronaves no tripuladas, UAS) y la responsabilidad civil**. El futuro de los UAS autónomos", cap. 20: Cuestiones clásicas y actuales del Derecho de daños, Vol. 1, 2021, págs. 889-950.

Impacto del sector

El progresivo incremento del nivel de automatización de las aeronaves no tripuladas, llegando incluso para algunos tipos de operaciones a la capacidad de operación completamente autónoma, es un factor disruptivo con un impacto transversal en el sector, desde los fabricantes de los sistemas hasta los proveedores de servicios y usuarios finales.

En las siguientes secciones se detallan los impactos esperados en los diferentes actores del ecosistema.

Operaciones y usuarios finales

Una de las principales barreras para la adopción de UAS por parte de los usuarios finales es la dificultad de escalar sus operaciones. Por esta razón, los principales casos de uso en la actualidad se limitan a aquellos en los que un uso puntual del UAS es suficiente y donde el piloto puede proporcionar toda la conciencia situacional necesaria. Para hacer económicamente viables muchas aplicaciones, desde la observación de la tierra hasta el transporte de mercancías con UAS, es necesario un cambio de paradigma en el que un solo operador pueda controlar múltiples UAS de forma completamente remota.

Pasar del paradigma "uno a uno" (un piloto controla un UAS) al "uno a varios" (un piloto controla múltiples UAS) requiere un nivel de automatización 4[30], donde el piloto monitoriza un sistema de alarmas mientras los UAS vuelan con el mayor grado de autonomía posible. Esto no solo permitirá reducir los costes operativos debido al aumento de la productividad de cada piloto, sino también mejorar la eficiencia de las operaciones, al no necesitar que el piloto esté en la misma ubicación que el UAS (evitando desplazamientos y permitiendo asignar recursos humanos y técnicos de forma flexible).

Escalar el número de operaciones gracias a la automatización también será el primer paso para disponer de datos suficientes que permitan optimizar las operaciones, incluyendo la optimización de rutas de vuelo y la aplicación de controles adaptativos en los UAS en función de las condiciones.

Una vez escalada la operación de UAS gracias a la automatización, se logrará no solo disponer de un medio de transporte autónomo más eficiente, seguro y sostenible que los utilizados actualmente, sino que también permitirá cambiar el paradigma de muchas aplicaciones, desde la captura de datos hasta el transporte de mercancías. Esto se logrará mediante el uso de vehículos con menor capacidad de carga pero con una mayor frecuencia y flexibilidad en las operaciones.

Proveedores de servicios

El avance en la autonomía de los drones está transformando la capacidad de las empresas de ofrecer nuevos servicios con mayores beneficios para sus clientes, en mercados donde incluso la regulación juega un hándicap respecto de los menos regulados. Sin embargo, aún queda un largo recorrido para satisfacer las necesidades de eficiencia, seguridad y capacidades que requiere el uso de esta tecnología a escala mundial.
Para que este nuevo paradigma de autonomía pueda trasladar todo su potencial desde los

[30] https://jarus-rpas.org/wp-content/uploads/2023/06/jar_21_doc_JARUS_Methodology_for_Evaluation_of_Automation_for_UAS_Operations.pdf

productos a los servicios, aún deben de desarrollarse nuevos tipos de servicios, fundamentales para dotar a los operadores de los UAS, de información geoespacial mejorada que ayude a los UAS a tener una mayor consciencia operacional, de nuevos servicios de coordinación de las operaciones dirigidas a operar bajo un "cielo único" (U-Space) con autorizaciones gestionadas "máquina a máquina", y de nuevos sistemas de información meteorológica capaces de prevenir condiciones ambientales desfavorables gracias a la toma de datos de las aeronaves ya en vuelo, entre otras.

Aún con la aparición de estos servicios, no se deben descuidar la mejora y optimización de otros servicios que se consideran críticos, como la mejora de los servicios para la navegación y posicionamiento que dependen en gran medida de infraestructuras gubernamentales, o la actualización periódica del espectro radioeléctrico, que permita alcanzar mayores distancias y mejores capacidades en materia de ciberseguridad.

Una vez hayamos madurado los servicios, las primeras misiones completamente autónomas se centrarán en casos de uso específicos y controlados, donde los drones requieran operar de manera segura y eficiente. Un ejemplo claro es la inspección de líneas de alta tensión, donde la alta recurrencia y homogeneidad de las operaciones permitirá llevar a cabo vuelos autónomos de manera sistemática. En general, cualquier tipo de trabajo recurrente sobre infraestructuras, sea de inspección, de monitorización o de vigilancia, tenderá a llevarse a cabo de manera desatendida por sistemas aéreos, principalmente por las cuestiones de inmovilidad y criticidad que les son inherentes frente a potenciales defectos o averías. Como consecuencia, la integración de nuevos servicios no solo va a producir un aumento drástico en la eficiencia de las operaciones, sino que se proporcionarán una reducción sobre los costes operativos, ya que no solo permitirá que operen vehículos más autónomos, sino que a su vez, cada uno de estos sistemas se empleará para múltiples misiones por vuelo.

Por otro lado, es esencial que los proveedores se mantengan al día con las regulaciones locales e internacionales para asegurar que sus servicios y tecnologías cumplan con los estándares requeridos. La disponibilidad oportuna de estas normativas es crucial, ya que la falta de claridad puede retrasar la implementación estas tecnologías en los mercados. Además, la adopción de estándares rigurosos de seguridad y privacidad es fundamental para proteger los datos y las operaciones de los drones autónomos. Esto incluye la implementación de medidas de ciberseguridad avanzadas y la garantía de que los datos recolectados se manejan de manera responsable y segura.

Fabricantes

El desarrollo y la integración de las capacidades de autonomía en los diferentes productos tiene también implicaciones muy relevantes para los todos fabricantes involucrados en la cadena de valor, desde fabricantes de equipos y componentes, pasando por fabricantes de sistemas, hasta integradores finales responsables del diseño completo de las aeronaves.

Las expectativas de la industria son de un crecimiento muy significativo en el mercado de las tecnologías relacionadas con el vuelo autónomo en las próximas décadas, pero esto requiere afrontar unos retos iniciales importantes.

Un aspecto clave en este sentido es la necesidad del desarrollo de nuevos sistemas y equipos que proporcionen las capacidades básicas habilitadoras para vuelo autónomo, como soluciones de Detect and Avoid para terreno, tráfico y obstáculos, o de despegue y aterrizaje autónomo, entre otras. La colaboración entre los fabricantes de estos sistemas y los fabricantes de aeronaves que los integran en sus productos es crucial para asegurar que las necesidades y prestaciones que unos

y otros pueden ofrecer son entendidas correctamente, y que los desarrollos avanzan en la misma dirección, maximizando las sinergias.

El desarrollo de estas nuevas capacidades exige a los fabricantes inversiones importantes en I+D, al tratarse de tecnologías en niveles de madurez bajos, y la adquisición de nuevos conocimientos y capacidades técnicas, bien mediante formación del personal existente o la contratación de nuevos perfiles especializados. Estos perfiles, relacionados con temas como el desarrollo software, la inteligencia artificial, los sensores avanzados o la computación de alto rendimiento, entre otros, son altamente demandados por diferentes industrias, lo que exige a los fabricantes del sector aeroespacial esfuerzos adicionales para conseguir atraer talento en un mercado laboral tan competitivo.

Como en el caso anterior para los operadores de servicios, los fabricantes se encuentran también con el problema de la falta de un marco regulatorio compatible con las nuevas tecnologías y paradigmas de vuelo autónomo. La regulación actual no puede dar una respuesta completa a estas necesidades, y las nuevas regulaciones aún están en proceso de definición. Esto deriva en una fuerte barrera de entrada para los fabricantes, especialmente para el caso de pequeñas y medianas empresas, que tienen que decidir si afrontar el riesgo de embarcarse en nuevos desarrollos con las inversiones y esfuerzos asociados mencionados sin la certeza de saber si sus productos podrán ser finalmente certificados, y en consecuencia, comercialmente viables. En este aspecto, la colaboración entre la industria y lo reguladores es de nuevo clave para avanzar de forma conjunta en la definición de una regulación que garantice que se cumple con los niveles de seguridad necesarios, y al mismo tiempo tenga en cuenta los aspectos intrínsecos de las tecnologías asociadas para asegurar que su aplicación es factible.

Todos estos retos son a la vez una gran oportunidad para la industria española del sector, que si es capaz de afrontarlos adecuadamente, puede capacitarse y posicionarse como un proveedor clave de productos y tecnologías de alto valor añadido en el mercado.

Desarrollo tecnológico y capacidades del sector

El avance hacia aeronaves altamente automatizadas (autónomas) representa un cambio significativo en el ecosistema. Los centros tecnológicos y universidades, como actores clave en el desarrollo tecnológico, enfrentarán impactos significativos que pueden ser tanto desafíos como oportunidades.

A continuación, se detallan los impactos esperados en estos actores:

Adquisición de Nuevas Capacidades en el Ecosistema

La automatización creciente en las aeronaves presenta una oportunidad única para que los centros tecnológicos y universidades fortalezcan y desarrollen el sector localmente, mediante por ejemplo su expansión tecnológica y operativa con el desarrollo de polos de movilidad aérea. En lugar de depender de potencias tecnológicas extranjeras, estas instituciones tendrán la oportunidad de liderar el desarrollo de nuevas tecnologías, adquiriendo capacidades en áreas como inteligencia artificial, robótica, sistemas de control autónomo y análisis de datos; fortaleciendo su competitividad y relevancia en el ámbito global.

Contribución de los Centros Tecnológicos y Universidades

Las universidades y centros tecnológicos serán los motores de la investigación, desarrollo e innovación (I+D+i), aportando investigación avanzada y desarrollando innovaciones que pueden ser llevadas a la industria para ser comercializadas por empresas del sector. Su contribución se extiende a la generación de publicaciones, patentes, prototipos y la realización de pruebas que validen nuevas tecnologías. La creación de laboratorios especializados en IA aplicada a UAS, robótica aérea, simulación de vuelo

autónomo y ciberseguridad para drones serán esenciales. Además, estas instituciones pueden ofrecer programas de formación continua para mantener actualizados a los profesionales del sector.
El sector espacial, que abarca la exploración espacial, los satélites y la astronáutica, está experimentando un rápido desarrollo y presenta una intersección significativa con el sector de aeronaves autónomas. El sector espacial ofrece una oportunidad estratégica para que los centros tecnológicos y universidades amplíen su alcance y lideren el desarrollo de tecnologías autónomas tanto en la Tierra como en el espacio. A través de inversiones en I+D, colaboración público-privada y desarrollo de nuevos perfiles profesionales, estas instituciones pueden posicionarse a la vanguardia de la innovación tecnológica en el sector espacial.

Inversiones Necesarias en I+D
Para aprovechar plenamente estas oportunidades, como en el caso de los fabricantes, se requerirán inversiones significativas en I+D. Estas inversiones deben enfocarse en infraestructura de laboratorio, adquisición de equipamiento de alta tecnología y contratación equipos de investigación y desarrollo especializados. El financiamiento de proyectos de investigación colaborativos con la industria también será vital para generar avances significativos y aplicables a corto y medio plazo.

Colaboraciones Público-Privadas, entre Centros Tecnológicos/Universidades e Industria y Soporte de las Administraciones Públicas
Para la financiación de proyectos, el apoyo de las administraciones públicas será fundamental. Las colaboraciones público-privadas, incluyendo las colaboraciones entre centros tecnológicos, universidades e industria, pueden impulsar la investigación y facilitar la transferencia de tecnología y conocimiento al sector industrial. Estas colaboraciones son esenciales para el desarrollo de tecnologías avanzadas y la formación de profesionales altamente cualificados. Los programas de subsidios, incentivos fiscales y creación de fondos específicos para la investigación en autonomía de aeronaves son ejemplos de soporte necesario. Además, el establecimiento de redes de colaboración entre universidades, centros tecnológicos y empresas fomentará un ecosistema robusto y dinámico.

Alternativas en la Regulación: Sandboxes
Para acelerar el desarrollo y experimentación de tecnologías autónomas, es crucial contar con un marco regulatorio flexible. La implementación de sandboxes regulatorios permitirá realizar vuelos experimentales en entornos controlados, reduciendo las barreras burocráticas y permitiendo pruebas más ágiles y seguras, antes de la puesta en servicio o acceso comercial de estos vehículos aéreos. Esto facilitará la validación de tecnologías emergentes y su posterior integración en el mercado[31].

Desarrollo de Nuevos Perfiles Profesionales
La evolución hacia sistemas 100% autónomos transformará el perfil profesional del sector. El rol del piloto de drones se adaptará hacia tareas de supervisión y gestión de flotas autónomas, requiriendo conocimientos avanzados en sistemas de control y análisis de datos. Igual que en el caso de los fabricantes, perfiles como ingenieros de sistemas autónomos, especialistas en inteligencia artificial aplicada a la navegación aérea y expertos en ciberseguridad para aeronaves serán altamente demandados. La formación en habilidades interdisciplinares, combinando conocimientos en aeronáutica, robótica y software, será clave para el futuro, con un enfoque en programas que combinen teoría y práctica, incluyendo simulaciones y prácticas en entornos reales.
El sector espacial ofrece oportunidades únicas para la formación y el desarrollo de habilidades. Los perfiles profesionales como ingenieros de sistemas espaciales, especialistas en telemetría y control de

[31] Sobre estas medidas para impulsar la innovación, pueden consultarse Bustos Moreno, Y.: "La responsabilidad civil en los espacios controlados de pruebas (regulatory sandboxes) sobre movilidad aérea urbana y la futura Ley de movilidad sostenible", *Cuadernos de Derecho Privado* 2 (2), 8-49; Bustos Moreno, Y.:"Análisis sobre las medidas de apoyo legal a la experimentación en tecnologías innovadoras", *Revista Española de Derecho Aeronáutico y Espacial*, n. 2, 2022, 319-346.

satélites y expertos en propulsión espacial serán cada vez más demandados.
En resumen, el incremento en la autonomía de las aeronaves ofrece una oportunidad estratégica para que los centros tecnológicos y universidades lideren el desarrollo del sector de drones y UAS. A través de inversiones en I+D, colaboración público-privada, marcos regulatorios flexibles y desarrollo de nuevos perfiles profesionales, estas instituciones pueden posicionarse a la vanguardia de la innovación tecnológica en aeronaves autónomas.

Aceptación social de las operaciones de UAS autónomos

Los UAS/drones autónomos permitirán que las aeronaves no tripuladas pasen a ser herramientas especializadas a activos indispensables en diversas industrias debido a su capacidad para mejorar la eficiencia, la seguridad y los costes en las operaciones. Sin embargo, los avances tecnológicos no son suficientes, ya que su aceptación por parte de la sociedad será crucial para hacer uso de todo su potencial.

A pesar de las grandes ventajas potenciales, la adopción de drones sigue siendo limitada, con tasas de aceptación que suelen rondar el 50 %. Los estudios[32] muestran que hay varios factores que influyen en la aceptación pública, como el ruido, la contaminación visual, la privacidad y la autonomía. Si bien los tres primeros aspectos son variables que pueden neutralizarse mediante avances en la tecnología o conceptos operativos, la aceptación de la autonomía está en gran medida influenciada por la actitud y el comportamiento de los individuos hacia esta tecnología[33].

Es importante señalar que, aunque esta percepción se basa en inputs subjetivos, ciertos factores cognitivos como la ventaja comparativa, la compatibilidad y factores emocionales como el beneficio social de las operaciones autónomas afectan indirectamente a la aceptación a través de su influencia en estas actitudes e intenciones de comportamiento.

Por lo tanto, son importantes estrategias específicas de comunicación, educación y desarrollo de infraestructura para mejorar la confianza en los UAS autónomos y, en consecuencia, la aceptación pública de las operaciones de UAS altamente automatizados. Al abordar eficazmente las preocupaciones y enfatizar los beneficios, las partes interesadas pueden crear un entorno propicio para la adopción generalizada de este tipo de tecnologías.

[32] https://www.sciencedirect.com/science/article/pii/S235214652200727X#:~:text=In%20recent%20years%2C%20civil%20drones,rates%20usually%20ranging%20around%2050%25.

[33] https://www.mdpi.com/2504-446X/8/3/107

Acrónimos

EASA	European Union Aviation Safety Agency
eVTOL	electrical Vertical Take-Off and Landing
GNSS	Global Navigation Satellite System
HWIL	HardWare In the Loop
IA	Inteligencia Artificial
IAM	Innovative Air Mobility
IMU	Inertial Measurement Unit
JARUS	Joint Authorities for Rulemaking on Unmanned Systems
ML	Machine Learning
LiDAR	Light Detection and Ranging
PAE	Plataforma tecnológica Aeroespacial Española
SORA	Specific Operations Risk Assessment
SWIL	SoftWare In the Loop
UAS	Unmanned Aerial System
UTM	Unmanned Traffic Management
VLL	Very Low Level