



NICOLLE LAFOSSE
Abogada Diaz Reus

¿QUIÉN VIGILA AL DRON? PRIVACIDAD, SEGURIDAD Y RESPONSABILIDAD LEGAL

Esta conversación analiza los principales desafíos legales que plantea el creciente uso de drones, desde la privacidad y la protección de datos hasta la seguridad, la vigilancia y la responsabilidad frente a posibles daños.

A medida que esta tecnología se integra en más operaciones empresariales, comprender sus implicaciones legales resulta fundamental para empresas, operadores y usuarios.



¿Quién vigila al dron? Privacidad, seguridad y responsabilidad en la era de los vuelos autónomos

Por Diaz Reus International Law Firm

Los drones ya no se limitan a la fotografía recreativa ni a aplicaciones aeronáuticas especializadas. Cada vez se utilizan más en ámbitos como la seguridad, la vigilancia, la inspección de infraestructuras, la agricultura, el sector inmobiliario, la logística y otras aplicaciones comerciales.

La expansión de sus capacidades, especialmente cuando se combinan con la inteligencia artificial y los sistemas autónomos, está planteando una cuestión jurídica cada vez más compleja: el hecho de que un dron pueda observar, grabar, recopilar información o tomar decisiones operativas no significa necesariamente que todos los usos de dichas capacidades sean legalmente permisibles.

En una reciente conversación de Diaz Reus, Nicole Lafosse, abogada especializada en tecnologías emergentes y con experiencia en derecho internacional, analizó la evolución del marco jurídico aplicable a los drones y la interacción entre la normativa aeronáutica, la privacidad, la protección de datos, la ciberseguridad y la responsabilidad jurídica.

Su análisis pone de relieve un desafío fundamental para las empresas: regular el vuelo es solo una parte de la ecuación. Las organizaciones también deben considerar qué capta un dron, cómo se utiliza esa información, quién controla la tecnología y quién podría ser, en última instancia, responsable cuando algo sale mal.

Los drones plantean un desafío regulatorio diferente

A diferencia de algunas tecnologías emergentes, los drones ya operan dentro de un marco normativo aeronáutico establecido. En Estados Unidos, la Administración Federal de Aviación (Federal Aviation Administration, FAA) regula el espacio aéreo nacional y establece las normas que rigen las operaciones con drones.

Sin embargo, contar con un organismo regulador aeronáutico claramente identificado no elimina la incertidumbre jurídica.

Como explicó Lafosse durante la conversación, algunas de las cuestiones más relevantes aún no resueltas en torno a los drones se agrupan en cinco grandes categorías: privacidad, responsabilidad por operaciones autónomas, tensiones jurisdiccionales entre las autoridades federales, estatales y locales, facultades en materia de sistemas antidrones, y seguridad de la cadena de suministro y de los datos.

Esta fragmentación es relevante porque una sola operación con drones puede involucrar diferentes ámbitos del derecho.

La FAA puede regular si una aeronave puede operar en el espacio aéreo y de qué manera, mientras que otras autoridades federales o estatales pueden intervenir cuando ese mismo dron graba a personas, recopila información sobre su ubicación, supervisa a empleados, causa daños materiales o trata datos personales.

Por tanto, para las empresas, el cumplimiento normativo no puede terminar simplemente con obtener autorización para volar.

El dron puede estar sujeto a una regulación diferente de la aplicable a los datos que recopila

Una de las distinciones más importantes abordadas durante la entrevista fue la diferencia entre regular la aeronave y regular la información captada por ella.

Un dron puede recopilar vídeos, fotografías, audio, información de geolocalización, matrículas de vehículos y potencialmente otros datos identificables. Cuando estos conjuntos de datos se combinan con tecnologías como el reconocimiento facial o con bases de datos externas, unas imágenes aparentemente ordinarias pueden convertirse en información mucho más reveladora.

Lafosse ilustró esta distinción comparando una sola imagen de una persona caminando por una acera pública con una secuencia de grabaciones que muestran a esa persona entrando en un vehículo, saliendo de una vivienda y desplazándose por lugares identificables. Por separado, esas imágenes pueden revelar relativamente poco. Sin embargo, en conjunto, pueden crear una imagen detallada de las actividades y rutinas de una persona.

Esta distinción adquiere especial importancia a medida que los drones se vuelven más sofisticados.

La cuestión jurídica puede ya no limitarse a determinar si una persona era visible desde un lugar público. Las empresas también pueden tener que preguntarse qué información se recopiló, si las personas pueden ser identificadas, si se captaron datos de geolocalización o audio, durante cuánto tiempo se conservará la información, si se combinará con otros conjuntos de datos y qué pretende hacer finalmente la organización con ella.

Captar información y utilizarla no son lo mismo

Otra cuestión importante es la diferencia entre la recopilación incidental y el uso posterior de la información.

Los drones comerciales que realizan inspecciones, trabajos de cartografía, operaciones de seguridad o actividades logísticas pueden captar involuntariamente propiedades colindantes o personas que no eran el objeto previsto de la operación.

Según Lafosse, la finalidad y el uso posterior de esa información son consideraciones fundamentales. Una organización que registra información de manera incidental puede estar sujeta a un análisis jurídico diferente al de una organización que almacena, analiza, combina o reutiliza deliberadamente dicha información. Al mismo tiempo, alegar que la recopilación fue accidental no resuelve automáticamente la cuestión; además, puede resultar difícil determinar la intención.

Para las empresas, esto sugiere que la gobernanza de los drones debería abordar todo el ciclo de vida de los datos, y no limitarse a las operaciones de vuelo.

Las organizaciones deberían comprender por qué se recopila la información, qué categorías de datos pueden captarse, quién puede acceder a ellos, cómo se utilizarán, durante cuánto tiempo se conservarán y cuándo deberán eliminarse.

Cuando un dron causa daños, la responsabilidad puede convertirse en una cadena

La responsabilidad se vuelve aún más compleja cuando un dron causa lesiones físicas, daños materiales o recopila o utiliza información de manera indebida.

La pregunta natural es: ¿Quién es responsable?

¿El piloto? ¿El propietario? ¿La empresa que utiliza el dron? ¿El fabricante? ¿El desarrollador del software?

La respuesta de Lafosse fue que la responsabilidad puede involucrar potencialmente a múltiples participantes, dependiendo de la naturaleza y la causa del daño.

Los distintos actores pueden tener responsabilidades diferentes. Uno puede ser responsable del cumplimiento de la normativa aeronáutica, otro de las decisiones operativas, otro de equipos defectuosos y otro de la recopilación o el uso indebido de los datos. En incidentes de importancia, esto puede generar una cadena de posibles responsabilidades que debe reconstruirse mediante pruebas y análisis jurídico.

Para las empresas, esto hace que la asignación contractual de riesgos sea especialmente importante cuando las operaciones con drones involucran a pilotos externos, proveedores tecnológicos, proveedores de software, contratistas de mantenimiento o empresas encargadas del tratamiento de datos.

Los drones autónomos complican las normas tradicionales de responsabilidad

La inteligencia artificial plantea una cuestión aún más compleja.

Tradicionalmente, la legislación en materia de negligencia suele evaluar la conducta preguntando qué habría hecho una persona razonable en circunstancias comparables. Los drones autónomos complican este marco porque un algoritmo puede tomar una decisión operativa sin que un piloto humano controle la aeronave en tiempo real.

Lafosse identificó esta cuestión como una de las zonas grises que están surgiendo en el ámbito del derecho aplicable a los drones.

Si una persona supervisa, por ejemplo, varias aeronaves autónomas, determinar la responsabilidad por una decisión tomada de manera independiente por uno de los sistemas puede requerir examinar no solo al operador humano, sino también el software, los procedimientos operativos de la organización, el nivel de supervisión humana y las circunstancias que rodearon el incidente.

Esto plantea un desafío jurídico más amplio que comparten muchas tecnologías basadas en inteligencia artificial: los marcos jurídicos diseñados en torno a la toma de decisiones humanas deben tener cada vez más en cuenta sistemas capaces de actuar con distintos grados de autonomía.

La vigilancia en el lugar de trabajo plantea otro conjunto de cuestiones

Los drones también son cada vez más relevantes para la seguridad y la vigilancia corporativas.

Las empresas pueden utilizarlos para supervisar instalaciones, inspeccionar perímetros, proteger activos u observar zonas operativas. Sin embargo, la vigilancia también puede captar a empleados y terceros.

En este contexto, Lafosse destacó varias consideraciones prácticas: información, consentimiento, finalidad, conservación y naturaleza de la información recopilada.

Las organizaciones deberían comprender por qué es necesaria la vigilancia, qué registrará el dron, cómo se utilizará la información resultante, durante cuánto tiempo se conservará y si constituye información personal. Las expectativas de privacidad también pueden variar en función de si una persona se encuentra en un lugar de trabajo, en una vivienda privada o en otro entorno.

La conclusión más amplia es que sustituir una cámara de seguridad fija por una plataforma aérea móvil no elimina las obligaciones existentes en materia de privacidad. En determinadas circunstancias, la movilidad y las mayores capacidades de observación pueden hacer que la gobernanza sea aún más importante.

La entrevista también examinó sectores en los que los drones ya se están convirtiendo en herramientas habituales.

En el sector inmobiliario, la fotografía aérea puede captar inadvertidamente viviendas vecinas o personas en lugares donde esperan tener privacidad. En la agricultura, las empresas deben tener en cuenta los parámetros operativos, los permisos de vuelo, la ubicación, la altitud y el alcance de la actividad que se realiza.

Estos ejemplos ilustran por qué una única «política de drones» genérica puede resultar insuficiente.

El perfil de riesgo jurídico de un dron utilizado en operaciones agrícolas es fundamentalmente diferente del de un dron que supervisa a empleados, fotografía una propiedad residencial, inspecciona infraestructuras industriales o funciona de forma autónoma como parte de una flota.

Un mejor punto de partida: definir primero la finalidad

Una de las recomendaciones más prácticas de Lafosse fue abordar el cumplimiento normativo de los drones desde una perspectiva inversa.

En lugar de adquirir o desplegar un dron y determinar posteriormente qué normas son aplicables, una organización debería definir primero el objetivo que pretende alcanzar.

¿Qué hará el dron? ¿Dónde operará? ¿Qué información captará? ¿Grabará vídeo o audio? ¿Recopilará información de geolocalización? ¿Funcionará de manera autónoma? ¿Se almacenará o analizará la información?

Una vez respondidas estas preguntas, la organización puede trabajar de forma retrospectiva para determinar los permisos, las limitaciones, las consideraciones relativas a la privacidad, los requisitos operativos y los controles internos que puedan resultar aplicables.

Este enfoque basado en la finalidad resulta especialmente valioso para las empresas porque el riesgo asociado a los drones rara vez corresponde exclusivamente a un solo departamento. Dependiendo de la operación, pueden tener que participar los equipos jurídico, de cumplimiento normativo, ciberseguridad, privacidad, seguros, operaciones, compras y gobernanza de la información.

Es probable que el futuro de la regulación de los drones siga siendo multinivel

Es poco probable que el futuro marco regulatorio de los drones consista en una única norma integral.

Como señaló Lafosse, un dron combina múltiples componentes y actividades: hardware, software, recopilación de datos, vídeo, audio, aviación, derechos sobre la propiedad y, potencialmente, toma de decisiones autónoma. Por lo tanto, distintas consecuencias pueden activar diferentes regímenes jurídicos y requerir la intervención de distintas autoridades.

Esta complejidad aumentará a medida que los drones sean más autónomos y estén cada vez más integrados con la inteligencia artificial y otras tecnologías emergentes.

Para las empresas, esperar a que desaparezca toda incertidumbre regulatoria probablemente no sea una estrategia viable.

Un enfoque más práctico consiste en establecer mecanismos de gobernanza antes del despliegue: definir la finalidad empresarial, comprender los datos involucrados, determinar los requisitos operativos aplicables, establecer responsabilidades, evaluar las relaciones con terceros y mantener registros que permitan explicar cómo y por qué se tomaron determinadas decisiones.

De la autorización para volar a la autorización para utilizar

La cuestión jurídica central en torno a los drones está adquiriendo un alcance que va más allá de la aviación.

Una empresa puede estar autorizada para operar un dron y, aun así, enfrentarse a cuestiones independientes relacionadas con la privacidad, la vigilancia, el tratamiento de datos, la ciberseguridad, los derechos sobre la propiedad o la responsabilidad.

Esta distinción probablemente cobrará cada vez más importancia a medida que los drones evolucionen desde dispositivos controlados individualmente hacia sistemas interconectados y autónomos capaces de observar, analizar y actuar a gran escala.

Por tanto, la cuestión para las empresas ya no es simplemente: «¿Podemos volar este dron?».

También es:

¿Qué observará? ¿Qué información generará? ¿Qué haremos con esa información?
¿Quién controla sus decisiones? ¿Y quién será responsable si algo sale mal?

Estas son las cuestiones que deberían abordarse antes de que la aeronave llegue siquiera a despegar.