01673/15/EN
GT 231

Dictamen 01/2015 sobre la privacidad y la protección de datos en relación con la utilización de aviones no tripulados (drones)

Adoptado el martes, 16 de junio de 2015

EL GRUPO DE TRABAJO DE PROTECCIÓN DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES

establecido mediante la Directiva 95/46/CE del Parlamento Europeo y del Consejo del 24 de octubre de 1995,

teniendo en cuenta los artículos 29 y 30 de la misma,

teniendo en cuenta sus Normas de procedimiento,

HA ADOPTADO EL SIGUIENTE DICTAMEN:

Resumen y comentarios

En vista de la progresiva integración de los aviones no tripulados (drones) en el espacio aéreo civil europeo y el surgimiento de numerosas aplicaciones de dichos drones (entre ellas el ocio, los servicios, la fotografía, la logística y la vigilancia de infraestructuras), existe una necesidad real de centrarse en los desafíos que podría plantear para la privacidad de las personas y las libertades civiles y políticas un despliegue a gran escala de la tecnología de aviones no tripulados y sensores, así como de evaluar las medidas necesarias para garantizar el respeto de los derechos fundamentales y la protección de los datos.

En efecto, pueden darse varios riesgos en relación con el tratamiento de datos (tales como imágenes, sonido y geolocalización relacionados con una persona física identificada o identificable) llevado a cabo por los equipos a bordo de un dron. Dichos riesgos pueden ir desde la falta de transparencia sobre los tipos de tratamiento realizado debido a la dificultad de ver los drones desde el suelo hasta, en todos los casos, la dificultad de saber qué tipo de tratamiento de datos hay a bordo, con qué fines se están recopilando datos personales y por parte de quién. Además, la destreza de los drones y la posibilidad de interconectar múltiples drones facilita aún más su capacidad de alcanzar puntos de observación únicos, por ejemplo evitando obstáculos o no viéndose limitados por barreras, muros o vallas, para permitir fácilmente recabar una gran variedad de información incluso sin necesitar una línea directa de visión durante periodos de tiempo largos y en grandes extensiones sin interrupción (con un riesgo elevado de recabación de grandes volúmenes de datos y posibles usos ilícitos con múltiples fines).

Se dan incluso riesgos mayores para los derechos y las libertades de las personas cuando el tratamiento de datos personales mediante aviones no tripulados (drones) se lleva a cabo con fines policiales.

Con el fin de abordar adecuadamente estas preocupaciones, tras haber aclarado el alcance del dictamen a la luz de las exenciones dispuestas en la Directiva 95/46/CE (exención doméstica, tratamiento con fines periodísticos y con fines policiales), el dictamen ofrece directrices para abordar correctamente las normas de protección de datos en el contexto de los drones.

Verificar la necesidad de una autorización específica de las autoridades de aviación civil (AAC) cuando la legislación nacional permite operar un dron, encontrar los criterios más adecuados para el tratamiento legítimo, cumplir con los principios de limitación de fines, minimización de los datos y proporcionalidad (eligiendo la tecnología más proporcionada y medidas que eviten la recogida de datos personales innecesarios) y cumplir, de la manera más apropiada para el caso que nos ocupa, con el principio de transparencia (informando a los interesados del tratamiento llevado a cabo) son obligaciones que deben cumplirse antes de operar un avión no tripulado. Asimismo es necesario adoptar todas las medidas de seguridad adecuadas y borrar o anonimizar aquellos datos personales que no sean estrictamente necesarios.

Además, el Grupo de Trabajo del Artículo 29 (GT 29) recomienda adoptar las medidas de privacidad por diseño y privacidad por defecto, y sugiere la evaluación de impacto sobre la protección de datos como una herramienta adecuada para evaluar el impacto de la aplicación de la tecnología de aviones no tripulados (drones) sobre el derecho a la privacidad y la protección de datos. Por otra parte, para aumentar la concienciación entre los usuarios se propone una recomendación específica a los fabricantes de drones de ofrecer suficiente información en los paquetes (por ejemplo dentro de las instrucciones de manejo) relativa a la intrusividad potencial de estas tecnologías y, donde sea posible, mapas que identifiquen claramente dónde se permite su uso.

Entre otros aspectos, el dictamen aborda también recomendaciones a los responsables normativos

europeos y nacionales para el fortalecimiento de un marco que garantice el respeto de todos los derechos fundamentales en juego, no solo la protección de datos, sino también para la introducción de normas específicas que garanticen un uso responsable de los drones (que debe incluir necesariamente el respeto de las áreas privadas). Además, el GT 29 solicita a los responsables normativos que introduzcan aspectos de protección de datos entre los elementos clave de las disposiciones nacionales que regulan el uso comercial de los drones (en conexión con la cualificación y formación de los pilotos, entre los requisitos de aeronavegabilidad y certificación, al emitir y revocar licencias operativas y permisos de trabajos aéreos), reclamando una cooperación escrita entre las autoridades de protección de datos y las AAC.

El GT 29 recomienda también a los fabricantes y operadores que incluyan opciones de diseño respetuosas con la privacidad y elementos de fábrica respetuosos con la privacidad como parte de un enfoque de privacidad por diseño y que incluyan a un delegado de la protección de datos (según disponibilidad) en el diseño y la implementación de políticas relacionadas con el uso de drones y, asimismo, promuevan la adopción de códigos de conducta que puedan ayudar a las diversas partes interesadas y operadores del sector a prevenir las infracciones y mejorar la aceptabilidad social de los drones. Asimismo, se establecen recomendaciones específicas para el uso de los datos personales recabados mediante aviones no tripulados (drones) con fines policiales. En concreto, el tratamiento de datos con fines policiales llevado a cabo mediante drones no debería por norma permitir el seguimiento constante y los equipos técnicos y de detección usados deben ser acordes con la finalidad del tratamiento.

1. Introducción

Con el fin de permitir la integración progresiva de los sistemas de aeronaves pilotadas de forma remota (RPAS, por sus siglas en inglés)[1] en el espacio aéreo civil[2], la Comisión Europea adoptó la comunicación COM(2014)207 «Una nueva era de la aviación. Abrir el mercado de la aviación al uso civil de sistemas de aeronaves pilotadas de forma remota de manera segura y sostenible», que responde al llamamiento del sector manufacturero y de servicios europeo a eliminar barreras a la introducción de los drones para uso civil en el mercado único europeo[3].

La apertura del mercado de drones requeriría la introducción de un marco regulatorio adecuado mediante la adopción, donde fuese necesario, de políticas nacionales y estándares europeos comunes, que debe desarrollar la Agencia de Seguridad de la Aviación Europea (EASA, por sus siglas en inglés). El Grupo de Trabajo del Artículo 29 (GT 29) señala, a ese respecto, la falta de un marco regulatorio adecuado en la mayoría de los Estados miembros. En este contexto, debe alentarse la armonización y modernización de las políticas de aviación de los Estados miembros en relación con los drones.

El GT 29 reconoce los beneficios sociales y económicos del uso civil de los drones, así como su potencial para el crecimiento y el empleo, pero considera igualmente importante poner de relieve todas las amenazas y riesgos para la protección de los datos y la privacidad derivados de un despliegue a gran escala de la tecnología de aviones no tripulados y evaluar las medidas necesarias para garantizar el respeto de todos los demás derechos fundamentales en juego[4].

Sin duda, el tratamiento de datos personales mediante drones tiene un carácter particular debido al punto de observación único que magnifica la efectividad de cualquier sensor a bordo e implica una menor transparencia y mayor intrusión en la privacidad en comparación con un sensor fijo similar, pese a sus similitudes aparentes –téngase en cuenta, por ejemplo, la vigilancia por vídeo mediante un dron frente al uso de una cámara de CCTV fija–.

La integración de los drones en el mercado de aviación europeo y sus diferentes propósitos civiles (entre ellos el uso policial) va a plantear desafíos específicos que deben superarse a fin de «respetar los derechos y principios consagrados en la Carta de los Derechos Fundamentales de la UE y en particular el derecho a la vida privada y la vida familiar (artículo 7) y la protección de los datos personales (artículo 8)»[5] y, en ese sentido, va a ser indispensable la implicación de los legisladores en el debate relativo a la integración de los drones en el espacio aéreo civil.

Conciliar todos los derechos e intereses en juego va a ser un reto que no pueden ignorar los responsables normativos a fin de garantizar que Europa esté en primera línea en este nuevo sector sin olvidar que «la Unión está fundamentada en los valores indivisibles y universales de la dignidad humana, la libertad, la igualdad y la solidaridad [y] en los principios de la democracia y el Estado de derecho»[6].

---

[1] Los sistemas de aeronaves pilotadas de forma remota son una subcategoría de las aeronaves no tripuladas, comúnmente conocidas como drones. Está definida por la OACI, sistemas de aeronaves no tripuladas (UAS, por sus siglas en inglés), número de orden: CIR328, 2011, Glosario, como «una aeronave en la que el piloto que la maneja no se halla a bordo de la misma». En aras de la simplicidad, el término *dron* se va a usar a lo largo de este dictamen como un término englobador para referirse a dichos sistemas.

[2] Véase Consejo Europeo, Conclusiones: 19/20 diciembre 2013, Euco 217/13.

[3] Debe recordarse que hay un proceso similar en marcha en los Estados Unidos. Para un resumen actualizado de las diferentes medidas adoptadas por la Administración Federal de Aviación en este campo véase https://www.faa.gov/uas/.

[4] Como son la dignidad humana, el derecho a la libertad y la seguridad, la libertad de pensamiento, conciencia y religión, la libertad de expresión e información, la libertad de reunión y de asociación y el derecho a la no discriminación.

[5] Documento de trabajo de los Servicios de la Comisión Europea *Towards a European strategy for the development of civil applications of Remotely Piloted Aircraft Systems (RPAS)* [Hacia una estrategia europea para el desarrollo de aplicaciones civiles de los sistemas de aeronaves pilotadas de forma remota], SWD(2012)259 final, 4 de septiembre de 2012, pág. 21. Para un reconocimiento de la necesidad de una «evaluación amplia de las amenazas a la privacidad» asociadas al uso de los drones, véase también el Grupo Director del RPAS Europeo, «Hoja de ruta para la integración segura de los RPAS civiles en el sistema europeo de aviación», 20 de junio de 2013, y su anexo 3, «Estudio sobre el impacto social», pág. 28. Los aspectos de privacidad de la aplicación de los drones se tomaron también en consideración en el reciente Dictamen sobre la ética de las tecnologías de seguridad y vigilancia presentado a la Comisión Europea por el Grupo Europeo de Ética de la Ciencia y de las Nuevas Tecnologías el 20 de mayo de 2014.

El presente dictamen responde al llamamiento hecho por la Comisión Europea[7] con el fin de ofrecer indicaciones prácticas a los legisladores y reguladores (tanto en el ámbito europeo como en el nacional, inclusive las Autoridades de Aviación Civil (AAC)[8]), la industria, los funcionarios responsables de las políticas y el público en general. Esto incluye abordar el impacto sobre la privacidad y la protección de datos así como las consecuencias del uso extendido de las diferentes aplicaciones de los drones para sus múltiples usos civiles. Se examinan también las peculiaridades y criticidades relacionadas con los requisitos específicos según el actual marco jurídico de la protección de datos. El Dictamen concluye con recomendaciones sobre el modo de abordar adecuadamente los riesgos que pueden surgir en relación con los drones y los propósitos para los que se usan para que el tratamiento de datos personales sea legal y cumpla con el marco jurídico de la protección de datos.

2. Descripción del fenómeno y de su repercusión en la privacidad y en la protección de datos

2.1 Definición, características y potencialidades de los drones

Según la Organización de Aviación Civil Internacional (OACI), un sistema de aeronave pilotada de forma remota (al que aquí se refiere como dron) es «un conjunto de elementos configurables consistente en una aeronave pilotada de forma remota, su estación o estaciones de pilotaje a distancia asociadas, los enlaces de mando y control necesarios y cualquier otro elemento de sistema que pueda requerirse en cualquier momento de la operación de vuelo»[9].

Por lo general, los drones son vehículos aéreos que pueden pertenecer a diferentes categorías con una gran variedad de especificaciones, características y capacidades[10]. Los drones pueden diseñarse para soportar distintas cargas útiles, por lo que sus tamaños y capacidad técnica son diversos. El tipo de dron más básico, que consta solo de componentes vitales[11], puede que no haga tratamiento de datos personales, pero aun así causa molestias y alarma social a otras personas. Añadir otros sensores para otros fines como son grabar datos de audio o vídeo plantea preocupaciones obvias relativas a la protección de datos y la privacidad. Es importante recordar no obstante que los drones disponibles comercialmente no vienen necesariamente equipados de fábrica con cámaras de a bordo u otros sensores y depende del operador el incluir o no tal capacidad, dependiendo del tipo de uso. Un dron puede también ser diseñado y construido por el propio operador obteniendo los componentes de distintos proveedores.

Algunos ejemplos de equipos que podrían afectar a la privacidad y la protección de datos son los siguientes:

- Equipos de grabación visual: cámaras inteligentes con distancia focal fija o variable, capaces de almacenar y transmitir imágenes en vivo, con capacidades de reconocimiento facial a bordo o desde tierra, que permiten a los drones identificar y hacer el seguimiento de personas, objetos o situaciones concretos, identificar patrones de movimiento, leer matrículas de vehículos, proporcionando al mismo tiempo una visión de 360°, habilitadas para detectar la energía térmica emitida por un objetivo, permitiendo el vuelo y la grabación de imágenes con malas condiciones de visibilidad (debido a niebla, humo o residuos) o en horas nocturnas;

---

[6] Carta de los Derechos Fundamentales de la Unión Europea, preámbulo.

[7] El 6 de mayo de 2014, la Dirección General de Empresa e Industria de la Comisión Europea dirigió una carta al GT 29 invitando a las APD a emitir «recomendaciones sobre el modo de abordar los problemas de privacidad y protección de datos a escala europea y sobre las acciones que deberían llevarse a cabo para respaldar el establecimiento de un marco adecuado».

[8] La normativa de seguridad de los RPAS de gran tamaño (> 150 kg) es competencia de la EASA, mientras que la regulación de los RPAS ligeros (< 150 kg) es competencia de las AAC nacionales (véase el artículo 4(4) y el ANEXO II del Reglamento (CE) n.º 216/2008).

[9] OACI, sistemas de aeronaves no tripuladas (UAS, por sus siglas en inglés), número de orden: CIR328, 2011, Glosario.

[10] Sus dimensiones pueden oscilar entre unos pocos centímetros y varios metros, y sus envolventes de vuelo pueden ser también muy diferentes, incluyendo capacidades de vuelo lento y planeo como muchos aerogiros u operaciones de alta velocidad y gran altitud como las aeronaves de alto rendimiento. El control de los drones mediante pilotajes remotos suele basarse en múltiples enlaces de datos y enlaces de mando proporcionados por equipos de radio o por enlaces de datos establecidos a través de Internet mediante enlaces de acceso inalámbrico digital, con pilotos a distancia trabajando sobre el terreno (o a bordo de otro vehículo), en muchos casos en su línea de visión. Para operaciones más allá de la línea de visión de un sistema de navegación, se requiere estrictamente confiar en sistemas de posicionamiento como GPS y equipos de telemetría para el conocimiento de posición del piloto durante el vuelo, enriquecido a veces con imágenes en vivo desde cámaras a bordo.

[11] P. ej. bastidor, motores, rotores, batería, receptor y controlador de vuelo.

- Equipos de detección: sensores optoelectrónicos, escáneres infrarrojos, radares de apertura sintética para identificar objetos, vehículos y embarcaciones y obtener información sobre su posición y curso incluso detrás de paredes, humo u otros obstáculos;
- Equipos de radiofrecuencia: tales como antenas que captan la ubicación de puntos de acceso wifi o estaciones celulares, femtoceldas y captador de IMSI usados por organismos policiales para controlar teléfonos y redes móviles o por el proveedor de servicios para la retransmisión de comunicaciones entre redes y usuarios de terminales;
- Sensores específicos para la detección de trazas nucleares, trazas biológicas, material explosivo y dispositivos explosivos.

Además, el grado en el que pueden modificarse los drones y adaptarse a situaciones específicas así como su bajo coste relativo están dando como resultado que los drones se apliquen a una serie de supuestos nuevos[12]. No obstante, en cualquier caso debe quedar claro que la cuestión pertinente desde el punto de vista de la privacidad y la protección de datos no es el uso de los drones en sí sino los equipos de tratamiento de datos a bordo de los drones y el consiguiente tratamiento de datos personales que puede producirse. De hecho, el tratamiento de imágenes (incluyendo imágenes de personas, casas, vehículos, matrículas, etcétera), sonido, datos de geolocalización o cualquier otra señal electromagnética relacionados con personas físicas identificadas o identificables llevado a cabo por los equipos de tratamiento de datos a bordo de un dron es lo que puede afectar a la privacidad y la protección de datos y, por lo tanto, suscitar la aplicación de la legislación de protección de datos[13].

2.2 Riesgos para la protección de datos

A la luz de todas las aplicaciones existentes y otras en el futuro previsible, se han puesto de relieve ya varios riesgos en cuanto a seguridad, responsabilidad de terceros y privacidad[14]. De hecho, por lo que respecta a este último aspecto, es probable, en una serie de casos, que los interesados no sean conscientes del dron o del tratamiento que se esté realizando de sus datos personales dado que estos dispositivos pueden ser difíciles de ver desde tierra. En cualquier caso, incluso si las personas son conscientes de que hay un dron en la zona, es difícil saber qué equipos de tratamiento de datos lleva a bordo, con qué fines se están recopilando y por parte de quién. Esto va a producir una mayor sensación de encontrarse vigilado y la consiguiente disminución posible del ejercicio legítimo de las libertades y derechos civiles, que se conoce como «efecto desalentador»[15].

---

[12] Su despliegue en operaciones tediosas, sucias o peligrosas es sumamente atractivo desde un punto de vista de la salud y la seguridad, dado que el operador humano puede permanecer a cierta distancia de la ubicación peligrosa. Por lo tanto, los drones pueden usarse en campos tradicionales de trabajo aéreo como son la vigilancia, el reconocimiento, la búsqueda y rescate, el control medioambiental, la agricultura, y también en otras áreas relacionadas con el entretenimiento y los deportes, el periodismo y las noticias, los documentales, la logística y transporte, la construcción y las obras públicas, la supervisión y el mantenimiento de redes e infraestructuras, así como con fines policiales.

[13] Véase, a este respecto, la definición de «datos personales» y «tratamiento de datos» contenida en los artículos 2(a) y 2(b) de la Directiva 95/46/CE. Debe hacerse hincapié en que la recopilación de datos sin grabación o almacenamiento es no obstante una operación de tratamiento que supone la aplicación de la legislación de protección de datos y que «la identificabilidad en el sentido expuesto en la Directiva puede ser resultado también de cruzar los datos con información en poder de terceros, o bien de la aplicación, en cada caso concreto, de técnicas y/o dispositivos específicos» (Grupo de Trabajo del Artículo 29 sobre Protección de Datos, Dictamen 4/2004 sobre el tratamiento de datos personales mediante videovigilancia, GT 89, p. 15). Para directrices amplias sobre la interpretación de la noción de datos personales, véase el Dictamen 4/2007 del Grupo de Trabajo del Artículo 29 sobre Protección de Datos sobre el concepto de datos personales, GT 136.

[14] Entre otros, véase el documento antes referido «Estudio sobre el impacto social», anexo a la «Hoja de ruta para la integración de los sistemas de aeronaves pilotadas de forma remota (RPAS) en el sistema europeo de aviación», y en otros lugares.

[15] Sobre el síndrome de efecto desalentador y panóptico derivado de un uso a gran escala de los drones, véase Rachel L. Finn, David Wright y Anna Donovan (Trilateral Research & Consulting, LLP), Laura Jacques y Paul De Hert (Universidad Libre de Bruselas), *Privacy, data protection and ethical risks in civil RPAS operations*, 7 de noviembre de 2014, en http://ec.europa.eu/DocsRoom/documents/7662, p. 28 y sig. y en otros lugares.

La destreza de los drones facilita aún más su capacidad de alcanzar puntos de observación únicos, por ejemplo para evitar obstáculos y no verse limitados por barreras, muros o vallas. Los drones pueden, por lo tanto, entrar más fácilmente en lugares privados, lo que facilita la recabación de una gran variedad de información de múltiples fuentes. En función de las tecnologías a bordo, los datos podrían obtenerse sin necesidad de una línea de visión directa (es decir, a través de tejados, residuos o nubes), durante periodos de tiempo largos y en grandes extensiones sin interrupción (con riesgo elevado de recogida de datos masivos y posibles usos múltiples ilícitos).

Se puede considerar también la posibilidad de interconectar una serie de drones para llevar a cabo vigilancia en un área extensa. Los enjambres de drones, con canales de comunicación en tiempo real entre ellos y con partes externas, suscitan aún mayores riesgos para la protección de datos, ya que podrían permitir fácilmente una vigilancia coordinada, es decir, rastreando movimientos de personas o vehículos en grandes extensiones.

Así pues, existe un riesgo elevado de que el tratamiento de datos personales con drones se convierta en una actividad encubierta y cause una interferencia grave en la esfera más íntima de las personas. Al mismo tiempo, existe un innegable riesgo aumentado de desviación de uso (es decir, riesgos de cambios o extensión de uso para fines incompatibles), teniendo en cuenta los equipos potencialmente sofisticados a bordo y la facilidad con la que los datos personales recopilados pueden vincularse con otra información.

Además, el impacto potencial de la intrusión en la privacidad se ve agravado por la gran diversidad de partes interesadas y entidades implicadas en su uso. Los fabricantes de drones, por ejemplo, tienen también un papel que desempeñar en la fase de diseño de los drones, ya que las características operativas pueden, en mayor o menor grado, prestarse a aplicaciones que interfieren en la intimidad (por ejemplo en el caso de drones pequeños o microdrones capaces de volar dentro de edificios).

La percepción de los drones por parte de las personas es inseparable de su sostenibilidad social. En este sentido, la aplicación efectiva del derecho de protección de datos puede contribuir a la aceptación de los drones. Por consiguiente, el GT 29 alienta las iniciativas y los proyectos de concienciación que acompañan la introducción de los drones en el mercado civil de la UE.

3. Análisis jurídico

Aunque no existe una legislación específica sobre las implicaciones para la protección de datos del uso de drones en los Estados miembros, el marco jurídico pertinente está constituido por la Directiva de Protección de Datos 95/46/CE (en adelante la Directiva) y, en la medida en que los drones pueden ser utilizados también por proveedores de servicios de comunicaciones electrónicas a disposición pública (p. ej. para ampliar el alcance de tales servicios), por la Directiva 2002/58/CE, modificada por la 2009/136/CE.

Por otra parte, a pesar de las diversas repercusiones que puede tener el uso de los drones sobre la privacidad y la libertad de las personas, en comparación con los sistemas de CCTV, podría haber circunstancias en las que las disposiciones legales nacionales aplicables a los sistemas de CCTV sean también aplicables al uso de los drones, en especial en caso de drones utilizados con fines de videovigilancia. En vista de ello, el GT 29 desea remitirse a su dictamen sobre el tratamiento de datos personales mediante videovigilancia, resaltando la actualidad del análisis jurídico y las recomendaciones contenidos en el mismo[16].

No obstante, debido a las mencionadas peculiaridades y riesgos de las aplicaciones de los drones, el GT 29 considera importante ofrecer directrices específicas sobre cómo cumplir con las normas de protección de datos en este contexto.

[16] Grupo de Trabajo del Artículo 29 sobre Protección de Datos, Dictamen 4/2004 sobre el tratamiento de datos personales mediante videovigilancia, id.

Siendo este el marco, debe prestarse atención a la cuestión de la responsabilidad del tratamiento de datos, considerando en especial la amplia gama de servicios basados en drones que ya ofrecen empresas especializadas a las organizaciones públicas y privadas. En vista de ello, es de la máxima importancia que el responsable y el encargado del tratamiento se identifiquen claramente para cada tipo de operación con drones, especialmente evaluando los elementos esenciales para distinguir al responsable del tratamiento de otros actores[17]. Puede encontrarse una directriz clara para identificar las diferentes combinaciones de responsabilidades entre las distintas entidades implicadas en el tratamiento conjunto en el dictamen del GT 29 1/2010 sobre los conceptos de «responsable» y «encargado»[18].

3.1 Aplicabilidad de la Directiva sobre protección de datos

Si bien la Comisión Europea está centrando su atención en los aviones no tripulados pilotados de forma remota, el presente dictamen no diferencia entre los sistemas de aeronaves no tripuladas autónomas y no autónomas, considerando que este aspecto no es relevante por lo que se refiere a los problemas de protección de datos derivados del uso de esta clase de tecnología. Es más, las directrices deberían aplicarse –con los necesarios ajustes– al tratamiento de datos derivado del uso de cualquier clase de vehículo aéreo (tripulado o no tripulado, aeronáutico o espacial) para operaciones civiles.

No obstante, debe resaltarse que algunos casos de tratamiento de datos personales derivado del uso de drones para operaciones civiles pueden escapar al ámbito de aplicación de estas directrices, habida cuenta de las exenciones o derivaciones que, según la Directiva, pueden establecer los Estados miembros (véase, en particular, los artículos 3, 9 y 13).

Conforme al artículo 3.2 de la Directiva, el tratamiento de datos personales por parte de una persona física en el curso de una actividad puramente personal o doméstica quedará excluido del ámbito de aplicación del presente dictamen.

No obstante, la disposición contenida en el artículo 3.2 es una excepción y, como tal, debe interpretarse en sentido restrictivo. Por lo tanto, tal como considera el Tribunal Europeo de Justicia, la así llamada «exención doméstica» debe «interpretarse en el sentido de aquellas actividades que se llevan a cabo en el ámbito privado o familiar de las personas, lo que obviamente no es el caso con el tratamiento de datos personales consistente en la publicación en Internet de modo que tales datos queden accesibles para un número de personas indefinido»[19]. Además, si las operaciones de un dron y los equipos de a bordo son de tal naturaleza que den lugar a un sistema de videovigilancia, hasta el punto de que este suponga la grabación y el almacenamiento constantes de datos personales y cubra, «incluso parcialmente, un espacio público y, en consecuencia, esté dirigido hacia el exterior del entorno privado de la persona que realiza el tratamiento de los datos de ese modo, no puede considerarse una actividad puramente "personal o doméstica" a efectos de lo establecido por el artículo 3(2) de la Directiva 95/46»[20].

---

[17] Un responsable del tratamiento «determina los fines y medios del tratamiento de datos personales» (artículo 2d de la Directiva). «Encargado del tratamiento» se refiere a la persona natural o jurídica, autoridad pública, agencia o cualquier otro organismo que procese datos personales en nombre del responsable del tratamiento (artículo 2e de la Directiva). Por ejemplo, aunque este papel parece estar claro cuando el dron lo usa directamente una empresa que lo ha comprado para repartir paquetería (responsable), podría tratarse de un marco diferente si una empresa se compromete a cartografiar una zona para un operador de drones (en este caso la empresa es el responsable y el operador es el encargado).

[18] Grupo de Trabajo del Artículo 29 sobre Protección de Datos, Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento», GT 169.

[19] Tribunal de Justicia Europeo, sentencia en el asunto C-101/01, caso Bodil Lindqvist, 6 de noviembre de 2003, párr. 47.

[20] Tribunal de Justicia Europeo, sentencia en el asunto C-212/13, František Ryneš v Úřad pro ochranu osobních údajů, 11 de diciembre de 2014, párr. 33. Véase más adelante en este documento acerca de los requisitos que esta aplicación conllevará en cuanto a legalidad, proporcionalidad, transparencia, medidas de seguridad, etcétera, considerando que, según ha recordado el Tribunal de Justicia Europeo, «la aplicación de la Directiva 95/46 posibilita, donde sea pertinente, tener en cuenta –con arreglo, especialmente, a los artículos 7(f), 11(2) y 13(1)(d) y (g) de dicha directiva– los intereses legítimos del responsable del tratamiento, como son la protección de la propiedad, la salud y la vida de su familia y de sí mismo».

Asimismo, según el artículo 9 de la Directiva de Protección de Datos, los Estados miembros podrían aplicar exenciones o derogaciones de algunas de sus disposiciones[21] en caso de tratamiento de datos personales llevado a cabo exclusivamente con fines periodísticos o de expresión artística o literaria[22]. No obstante, las exenciones y derogaciones solo deben ser aquellas que sean «necesarias para conciliar el derecho a la privacidad con las normas que rigen la libertad de expresión».

Por consiguiente, el tratamiento de datos personales llevado cabo por medio de drones por motivos periodísticos debería tener en cuenta las diferentes legislaciones y disposiciones nacionales que se aplican a este tipo de tratamiento. En cualquier caso, los Estados miembros deben ser conscientes de la intrusividad potencial de estos instrumentos, especialmente si se usan de modo irresponsable y falto de ética, y deben identificar con claridad los deberes y las responsabilidades que lleva aparejado el ejercicio de la libertad de expresión con ayuda de drones.

El GT 29 confiere la máxima importancia a la introducción de un marco apropiado de ámbito nacional (si no existiese ya) de modo que el uso de los drones con fines estrictamente personales y recreativos y con fines periodísticos[23] no menoscabe los derechos fundamentales a la privacidad o la confidencialidad de las comunicaciones y pueda garantizarse el respeto de una expectativa razonable de protección de la vida privada incluso en caso de recopilación de datos personales llevado a cabo en lugares públicos. Tal como ha recordado el Tribunal Europeo de Derechos Humanos, existe «una zona de interacción de una persona con otras, incluso en un contexto público, que podría considerarse parte del ámbito de la vida privada»[24]. Por lo tanto, los legisladores y los reguladores (tanto de ámbito nacional como europeo) también deben tener en cuenta los principios generales y algunas sugerencias específicas expuestas en este dictamen cuando establezcan los requisitos que deben cumplirse para el uso de aeromodelos[25] y los que debe cumplir el público en general para evitar infringir la legislación de protección de datos y otras reglamentaciones nacionales de salvaguarda de otros derechos personales[26].

---

[21] En concreto, las relativas a las normas generales sobre la legalidad del tratamiento, las normas sobre transferencias a terceros países y las normas sobre autoridad supervisora y GT 29 (artículos 6 (1), 10, 11 (1), 12 y 21 de la Directiva).

[22] Una actividad podría clasificarse como periodística en tanto en cuanto su «objeto sea la divulgación al público de información, opiniones o ideas, independientemente del medio que se use para transmitirlas. No se limita a las empresas de medios de comunicación y puede hacerse con fines lucrativos» (Tribunal de Justicia Europeo, sentencia en el caso C-73/07, Tietosuojavaltuutettu contra Satakunnan Markkinapörssi Oy y Satamedia Oy, 16 de diciembre de 2008, párr. 61). De modo similar, el Tribunal Europeo de Derechos Humanos consideró que «la función de la prensa incluye la creación de foros para el debate público. No obstante, el desempeño de esta función no se limita a los medios de comunicación o los periodistas profesionales» (véase Tribunal Europeo de Derechos Humanos, sentencia en el caso Társaság a Szabadságjogokért contra Hungría, 14 de abril de 2009, párr. 27).

[23] A este respecto, por ejemplo, podría ser aconsejable la adopción del código de conducta periodístico para abordar este problema teniendo en cuenta todos los diferentes intereses en juego.

[24] Tribunal Europeo de Derechos Humanos, sentencia en el caso de Von Hannover contra Alemania (n. 2), 7 de febrero de 2012, párr. 95. Abundando en esta cuestión, véase Supervisor de Protección de Datos Europeo, Dictamen sobre la Comunicación «Una nueva era de la aviación. Abrir el mercado de la aviación al uso civil de sistemas de aeronaves pilotadas de forma remota de manera segura y sostenible», 26 de noviembre de 2014, pág. 7. Conciliando con cuidado los diferentes intereses en juego, los Estados miembros todos ellos Estados parte en la Convención Europea de Derechos Humanos– cumplirían también con la obligación de garantizar el respeto efectivo de la vida privada y familiar que se deriva del artículo 8 de la Convención (véase Tribunal Europeo de Derechos Humanos, –sentencia en el caso Aire y contra Irlanda, 9 de octubre de 1979, párr. 32, sentencia en el caso Marckx, 13 de junio de 1979, párr. 31).

[25] La anteriormente mencionada Circular 328 de la OACI (punto 2.4) recuerda que los aeromodelos se hallan fuera del ámbito de aplicación de las disposiciones de la Convención de Chicago, pero podrían ser objeto de reglamentaciones nacionales relevantes. En este marco, podría plantearse la introducción de normas específicas que garanticen un uso responsable de los drones, las cuales deben incluir necesariamente el respeto de las zonas privadas (tales como jardines, patios, terrazas, etcétera) y de una «expectativa razonable» de privacidad incluso en las zonas públicas; con ese fin, debería plantearse la introducción, cuando sea necesario, de perímetros virtuales. A este respecto, véase, por ejemplo, el Reglamento italiano sobre vehículos aéreos pilotados de forma remota (artículo 23).

[26] La distribución de un folleto que acompañe a cada aeromodelo comercializado, por ejemplo, podría ser útil para llamar la atención sobre el respeto necesario del principio de protección de datos, donde sea aplicable, y otras reglamentaciones nacionales. Puede verse un ejemplo interesante de estos folletos para el uso personal de drones (*Règles d'un bon usage d'un drone de loisir* [Normas para el buen uso de un dron con fines lúdicos]) en http://www.developpement- durable.gouv.fr/IMG/pdf/Drone-_Notice_securite-2.pdf. Véase también, a este respecto, la lista de acciones permitidas y prohibidas para los aeromodelos volantes emitida en los Estados Unidos por la FAA y publicada en http://www.faa.gov/uas/publications/model_aircraft_operators.

3.2 Tratamiento de datos personales con fines policiales

Los drones pueden suponer una transformación fundamental de las prácticas policiales, especialmente por lo que respecta al papel de los datos a la hora de orientar las acciones policiales, desde el seguimiento de personas hasta la determinación de objetivos a partir del examen de las vidas y actividades de una población específica basándose en la vigilancia continua. Así pues, el uso de drones directamente operados por la policía y otras fuerzas del orden público –o la solicitud por parte de estas de acceder a datos recopilados por drones operados por entidades privadas para sus propios fines– genera riesgos elevados para los derechos y libertades de las personas e interfiere directamente en los derechos al respeto de la vida privada y la protección de los datos personales protegidos en virtud del artículo 8 de la Convención Europea de Derechos Humanos (CEDH) y los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea (la «Carta»).

Por lo tanto, según el artículo 52(1) de la Carta y el artículo 8 (2) del CEDH, esta limitación al ejercicio de los derechos y libertades reconocidos por la Carta debe hacerse por ley («con arreglo a la ley»), solo si es necesario y satisface realmente los objetivos del interés general reconocidos por la Unión o responde a la necesidad de proteger los derechos y libertades de otros («en aras de alguno de los objetivos legítimos expuestos en el artículo 8 (2) del CEDH y necesarios en una sociedad democrática»).

En consecuencia, la policía y otras autoridades del orden público que utilizan drones deben asegurarse de que el tratamiento de datos personales que realizan cuenta con una base jurídica válida.

Los drones solo se usarán allí donde se ofrezca una demostración concreta de su necesidad y pertinencia para los fines específicos perseguidos. A este respecto, el GT 29 llama la atención sobre su dictamen 01/2014 sobre la aplicación de los conceptos de necesidad y proporcionalidad así como protección de datos en el ámbito policial.

Las mencionadas autoridades deberán justificar por qué no lograrían tales fines con los instrumentos con los que cuentan actualmente y con alternativas menos intrusivas (puede ser pertinente a estos efectos una evaluación previa por parte de las autoridades de protección de datos cuando las prácticas nacionales lo favorezcan).

Además, cuando las autoridades policiales procesen datos recabados por drones en persecución de delitos civiles, deberán cumplir con los requisitos establecidos por la Directiva. En concreto, tales usos de los drones deben limitarse a aquellos casos en los que el tratamiento sea necesario para proteger los intereses vitales del afectado o para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos.

Una vez que se haya determinado la necesidad del uso de drones para fines policiales o de orden público, según el artículo 52(1) de la Carta y el artículo 8 del CEDH, su uso deberá cumplir con el principio de proporcionalidad y con los requisitos específicos de protección de datos: no debe ir más allá de lo estrictamente necesario para cumplir con el objetivo legítimo que se persigue.

En este sentido, deben seguirse los principios establecidos en el Convenio n.º 108 del Consejo de Europa y la Recomendación R (87) 15 que regula el uso de datos personales en el ámbito policial, adoptado por el Comité de Ministros el 17 de septiembre de 1987, así como los principios pertinentes de la Decisión marco sobre protección de datos 977/2008.

Además, el GT 29 recuerda que el tratamiento de datos con drones llevado a cabo por servicios gubernamentales solo debe hacerse para los fines establecidos en la legislación correspondiente y no debe emplearse para vigilancia masiva, tratamiento de grandes volúmenes de datos, agrupamiento de datos y creación de perfiles: deben imponerse límites en el uso de drones para actividades de vigilancia con el fin de evitar que se hagan omnipresentes o se usen para señalar objetivos basándose en el análisis de datos. Por lo tanto, los drones solo deben usarse con los fines

estrictamente enunciados y justificados que puedan publicarse de antemano y, en cualquier caso, el uso debe limitarse a un ámbito geográfico y temporal. En vista del «efecto desalentador» que puede tener el uso de los drones sobre los derechos a la libertad de expresión y de reunión, debe prestarse atención en especial a la necesidad de proteger, en la medida de lo posible, las manifestaciones públicas y reuniones de similar naturaleza de cualquier tipo de vigilancia.

3.3 Legalidad del principio de limitación del tratamiento y los fines

Para que sea legal, el tratamiento de datos personales que conlleva la aplicación civil de la tecnología de drones debe basarse en uno de los criterios para considerar legítimo el tratamiento de datos que se hallan expuestos en el artículo 7 de la Directiva[27]. Recordando el dictamen sobre el interés legítimo que ofrece directrices amplias sobre este aspecto[28] y teniendo en cuenta las peculiaridades del tratamiento de datos personales llevado a cabo por medio de equipos a bordo de drones, varios fundamentos jurídicos se podrían considerar pertinentes de acuerdo con los diversos fines del tratamiento en juego:

- consentimiento libremente otorgado, específico e informado (art. 7a).
  Si bien el consentimiento es un fundamento jurídico común que resulta fiable, parece que en este contexto solo en pocos casos se podría considerar apropiado, especialmente cuando los datos se recaban en zonas públicas. El consentimiento en cualquier caso debe otorgarse libremente y ser específico e informado. En la mayoría de los casos en cuestión, sería muy difícil cumplir todos estos requisitos, ya que el consentimiento, por ejemplo, no sería «libremente otorgado» en tanto en cuanto la persona no fuese libre de acceder a o salir de una zona vigilada sin estar sometido a vigilancia; el consentimiento no será «informado» si a dicha persona no se le ofrece toda la información necesaria sobre el tratamiento, ni será «específico» si no es posible para la persona conocer cada propósito del tratamiento para el que se le pide consentimiento[29].
  El consentimiento podría ser un fundamento jurídico apropiado para el tratamiento de datos personales llevado a cabo por medio de una cámara a bordo de un dron por ejemplo en el caso de una sesión de entrenamiento de un equipo deportivo (es decir, sin la presencia de espectadores).
- tratamiento necesario para la ejecución de un contrato del que sea parte el interesado (art. 7b)
  El tratamiento de datos personales es legal de acuerdo con el artículo 7b de la Directiva, por ejemplo, cuando alguien adquiere un producto que el vendedor entrega en su domicilio mediante un dron, o bien cuando las empresas que operan los drones proponen servicios de videograbación solo dirigida a las propiedades de los interesados; no obstante, debe tenerse en cuenta que el tratamiento incidental de datos de terceros no afectados nunca está cubierto por el cumplimiento de obligaciones de las partes de un contrato y, por lo tanto, en los ejemplos referidos, debe evitarse la recopilación de datos de terceros o encontrar un fundamento jurídico diferente para legitimarla.
- el tratamiento es necesario para el cumplimiento de una obligación legal o necesario para el desarrollo de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos (arts. 7c y 7e)
  Estos fundamentos jurídicos podrían valer en los casos en los que el responsable del tratamiento deba cumplir con una obligación legal, como puede ser la vigilancia de un sitio arqueológico exigida por una disposición específica o, por ejemplo, en algunos «usos relacionados con la seguridad», como el control del contrabando, solo en aquellos casos en los que el uso de drones sea estrictamente necesario y proporcionado.
- el tratamiento es necesario para proteger los intereses vitales del interesado (art. 7d)

[27] No obstante, en todos los casos en los que el uso de drones pudiera conllevar el tratamiento de categorías especiales de datos, se aplicará el artículo 8 de la Directiva.
[28] Véase Grupo de Trabajo del Artículo 29 sobre Protección de Datos, Dictamen 06/2014 sobre la noción de intereses legítimos del responsable del tratamiento, GT 217, pág. 16 y sig.
[29] Véase Grupo de Trabajo del Artículo 29 sobre Protección de Datos, Dictamen 15/2011 sobre el consentimiento, GT 187.

Este fundamento jurídico podría ser pertinente en algunos casos de «usos relacionados con la seguridad» de un dron como puede ser ayuda en catástrofes, inspección de lugares incendiados, rescate de víctimas de avalanchas de nieve y accidentes de montaña, etcétera. No obstante, teniendo en cuenta que el artículo 7(d) debe interpretarse en sentido estricto, un mejor enfoque podría ser considerar estos usos en virtud de los artículos 7(c), 7(e) o 7(f), dependiendo de las circunstancias del caso[30].

- el tratamiento es necesario para fines de interés legítimo (art. 7f)
  Los datos personales pueden también procesarse si ello es necesario para los fines del interés legítimo perseguido por el responsable del tratamiento o por el tercero salvo cuando prevalezcan sobre tales intereses los intereses o los derechos y libertades fundamentales del interesado (es previsible que tales criterios sean aplicables, por ejemplo, en caso de operaciones de drones necesarias para inspección de tuberías o líneas eléctricas, o bien para vigilancia de infraestructuras clave o fotogrametría aérea, investigación atmosférica y meteorológica, control de energía eólica, seguimiento de huracanes, cartografiado de excavaciones arqueológicas, seguimiento de hielo marino o investigación de fauna y flora)[31], si se aplican en el sistema las salvaguardas apropiadas.

Además, y considerando uno de los riesgos antes mencionados que conlleva la recogida de una enorme cantidad de datos con las aplicaciones de drones y la así llamada «desviación de uso», debe recordarse que los datos personales deben recabarse con fines concretos, explícitos y legítimos y no se deben someter a tratamiento adicional de un modo que sea incompatible con tales fines (artículo 6.1.b de la Directiva)[32].

Por consiguiente, todo tratamiento adicional de datos personales para un fin diferente a aquel para el que se han recopilado los datos debe realizarse de acuerdo con las disposiciones de la Directiva y por lo tanto debe tener un fundamento jurídico autónomo, y su compatibilidad con el fin original debe también evaluarse caso por caso[33].

Además, de acuerdo con el principio de legalidad (artículo 6.1.a de la Directiva), cualquier operación con drones que implique el tratamiento de datos personales debe, en primer lugar, cumplir con la legislación aplicable en general[34], incluidos los reglamentos nacionales sobre CCTV y sobre el uso de drones[35].

3.4 Principios de proporcionalidad, calidad de los datos y minimización de los datos: el papel relevante de la privacidad por diseño y por defecto

Puesto que los datos personales solo pueden procesarse si son adecuados, pertinentes y no excesivos en relación con los fines para los que se recaban, debe tener lugar una evaluación estricta de la necesidad y la proporcionalidad de los datos procesados (artículo 6 de la Directiva). Los datos personales solo se procesarán en la medida en que los fines no se puedan cumplir mediante un tratamiento de información que no implique datos personales.

[30] Véase también Grupo de Trabajo del Artículo 29 sobre Protección de Datos, Dictamen 06/2014 sobre la noción de intereses legítimos del responsable del tratamiento, GT 217, págs. 20 y 21.

[31] Existen directrices útiles con respecto a este fundamento jurídico en el dictamen del GT 29 sobre el interés legítimo. Ibíd. No obstante, en vista de la potencial gravedad de la interferencia con la protección de datos y la privacidad de otras personas causada por el uso de drones, según el fallo del Tribunal de Justicia de la Unión Europea en el caso de Google España, parece evidente que dicho tratamiento está difícilmente justificado simplemente por el interés económico que tenga el responsable en el mismo (Tribunal de Justicia de la Unión Europea, sentencia en el caso C-131/12, Google Spain SL y Google Inc. contra la Agencia Española de Protección de Datos y Mario Costeja González, 13 de mayo de 2014, párr. 81).

[32] Así, por ejemplo, no debería ser posible el uso adicional de imágenes de terrenos agrícolas, captadas para asegurarse de que los pesticidas se diseminan adecuadamente, para grabar datos de terrenos y técnicas colindantes o para filmar un área para asegurarla y utilizar las imágenes o vídeos para multar a las personas que no han pagado entrada.

[33] Véase Grupo de Trabajo del Artículo 29 sobre Protección de Datos, Dictamen 03/2013 sobre limitación de fines, GT 203. Para otro ejemplo significativo de uso incompatible de datos personales, véase Grupo de Trabajo del Artículo 29 sobre Protección de Datos, Dictamen 10/2006 sobre el tratamiento de datos personales realizado por la Society for Worldwide Interbank Financial Telecommunication (SWIFT), GT 128, pág. 15. Además, el respeto del principio de limitación de finalidad es, por ejemplo, de importancia clave en caso de mutualización (véase anteriormente el párrafo 2.1.).

[34] Legislación sobre protección de datos y demás leyes aplicables, como la legislación nacional que salvaguarda los derechos personales, la imagen, la vida familiar y la esfera privada.

[35] Por estos motivos, en los Estados miembros en los que el manejo de drones incumple la normativa en materia de aviación nacional, se considerará que el tratamiento de datos personales recabados durante las operaciones no cumple con el principio de legalidad.

Además, el principio de minimización de datos podría respetarse eligiendo una tecnología proporcionada y adoptando medidas de protección de datos y privacidad por defecto, es decir, una configuración de privacidad de los servicios y los productos que por defecto evite la recabación y el tratamiento posterior de datos personales innecesarios[36]. Una carga útil menos intrusiva debería ser siempre la opción preferente y, siempre que sea apropiado, por ejemplo, podría plantearse la implementación de técnicas de anonimización –tal como se expone en el Dictamen 05/2014 sobre las técnicas de anonimización[37]– cuando el tratamiento de datos personales sea innecesario.

Además, en relación con las diversas tecnologías que pueden leer electrónicamente y procesar datos biométricos (reconocimiento facial, identificación de comportamientos), puede verse un análisis actualizado con aclaraciones y recomendaciones útiles en el dictamen del GT 29 sobre los desarrollos en tecnologías biométricas[38]. Por ejemplo, cuando se usen drones equipados con videocámaras, los responsables del tratamiento podrían hacer ajustes técnicos para procesar automáticamente las imágenes con efectos de difuminación u otros efectos gráficos para evitar la recopilación de imágenes de personas identificables siempre que no sean necesarias.

La aplicación de medidas de protección de datos por defecto implica que los fabricantes y operadores respeten de antemano el principio de protección de datos por diseño. La protección de datos debe incorporarse en todo el ciclo de vida de la tecnología, desde la fase de diseño inicial hasta su despliegue último, el uso y su desechado final; dicha tecnología debe diseñarse de tal modo que se evite el tratamiento de datos personales innecesarios (por ejemplo, en caso de infraestructuras estratégicas o críticas, podría ser aconsejable diseñar el *firmware* de los drones de tal modo que se inhiba la recabación de datos dentro de zonas vetadas al vuelo previamente definidas)[39].

Dada la variedad de aplicaciones de los drones, para evaluar su impacto sobre los derechos y la libertad de las personas y en particular sobre el derecho a la privacidad y la protección de datos, podría llevarse a cabo una evaluación de impacto en la protección de datos. Su finalidad sería ayudar a los operadores a descubrir los riesgos para la privacidad (en su caso) asociados al uso de nuevas aplicaciones y evaluar si el tratamiento de datos personales mediante drones es legítimo, necesario y proporcional al fin perseguido, cubriendo al mismo tiempo, entre otras, cuestiones de transparencia y seguridad y documentando las medidas adoptadas para abordar esos riesgos[40].

En vista de ello, el GT 29 solicita a los responsables normativos competentes, tanto de ámbito europeo como nacional, que evalúen la oportunidad, al estudiar el nuevo marco legal para la integración de los drones en el espacio aéreo civil europeo, de promover la implementación, como práctica idónea, de una evaluación de impacto sobre la protección de datos para cada tipo de operación con drones que pueda suponer el tratamiento de datos personales habida cuenta de los riesgos previsibles derivados de las aplicaciones previstas, asimismo proporcionando a todos los actores (fabricantes y operadores) un conjunto de criterios de fácil aplicación.

---

[36] Por ejemplo, si se almacenan datos a bordo de un dispositivo deben eliminarse lo antes que sea razonablemente posible y el responsable del tratamiento debe conservarlos de forma segura de acuerdo con políticas de conservación claramente definidas. El almacenamiento a largo plazo de datos recopilados en un dispositivo se pone en riesgo innecesario de pérdida o robo en una misión de vuelo posterior. Por otra parte, los drones desplegados para la entrega de paquetería es improbable que deban estar equipados con cámaras con capacidades de reconocimiento facial o grabación de audio. Un dispositivo usado para supervisar daños por tormentas en tejados no debe necesitar realizar grabaciones durante todo el vuelo, especialmente si la ubicación de interés se halla a cierta distancia de la ubicación de despegue y aterrizaje. En este sentido, podría ser aconsejable involucrar al delegado de la protección de datos (donde se disponga del mismo) en el diseño y la implementación de políticas relativas al uso de los drones.

[37] Véase Grupo de Trabajo del Artículo 29 sobre Protección de Datos, Dictamen 05/2014 sobre las técnicas de anonimización, GT 216.

[38] Grupo de Trabajo del Artículo 29 sobre Protección de Datos, Dictamen 3/2012 sobre los desarrollos en las tecnologías biométricas, GT 193.

[39] La propuesta de la Comisión Europea para un reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, COM(2012) 11 final, prevé mecanismos para garantizar que, por defecto, solo se procesen aquellos datos personales que sean necesarios para cada finalidad específica del tratamiento y que no se recopilen especialmente datos ni se conserven más allá del tiempo mínimo necesario para tales fines (véase a este respecto el artículo 23).

[40] En este contexto, en primer lugar, para cada tipo de aplicación de drones, una evaluación previa debe tener en cuenta los tipos de datos necesarios y estándares que pueden recopilarse. Por ejemplo, la simple recopilación de datos relativos al vuelo del dron (tales como altitud, velocidad del aire, longitud del vuelo), puede que no implique automáticamente la aplicación de las obligaciones de protección de datos, a menos que el piloto u otra persona física sean identificables a partir de los datos (p. ej. el nombre del piloto o el número del empleado están incluidos en los metadatos de registro).

En especial, puesto que las normas de protección de datos deben respetarse en la medida en que se procesen datos personales, debe plantearse una evaluación de impacto sobre la privacidad y la protección de datos para los fabricantes en los casos de drones «diseñados y producidos» con fines de vigilancia y para operadores que usen drones que lleven a bordo cualquier tipo de equipos «audiovisuales», teniendo en cuenta, como se ha dicho antes, las cargas útiles y los propósitos de la recopilación y el tratamiento de datos personales ulterior[41].

En los casos en los que los drones cuenten con un sistema de reconocimiento de imágenes, debería considerarse la implementación de un mecanismo que facilite el ejercicio de la objeción del interesado en forma de etiquetas activas o pasivas que comunicarían claramente las intenciones de los interesados frente al tratamiento de su imagen o los dispositivos usados por estos como etiquetas visuales usadas en ese momento cuyo objetivo sea mostrar a los fotógrafos en conferencias públicas de qué modo puede usarse la imagen de las personas fotografiadas[42].

3.5 Transparencia e información para con los interesados

Conforme al principio de tratamiento justo (artículo 6(a) de la Directiva), los interesados deben ser conscientes de la recabación y el tratamiento de sus datos personales y por lo tanto se les debe informar de conformidad con el artículo 10 de la Directiva, sin perjuicio de las exenciones previstas en los artículos 11 y 13. Lo antes que sea razonablemente posible y si se prevé una revelación a un tercero, a lo sumo cuando los datos se revelen en primer lugar, de conformidad con el artículo 11 de la Directiva, se deberá ofrecer a los interesados la siguiente información: la identidad del responsable del dron y su representante, los fines de tratamiento para el que están previstos los datos, cualquier información adicional, como pueden ser las categorías de datos, los destinatarios o las categorías de destinatarios de los datos, la existencia del derecho de acceso y el derecho a especificar y corregir los datos que les afectan.

Para cumplir estos requisitos de transparencia e información a los interesados, los responsables del tratamiento deberían considerar un enfoque de canales múltiples[43]. Las disposiciones habituales como son señalizaciones u hojas informativas para un acontecimiento (p. ej. para un paquete de entrada a una regata de remo) o en la información sobre acontecimientos (p. ej. un programa deportivo) podrían aplicarse con facilidad en las operaciones con drones en ubicaciones fijas (con ocasión de acontecimientos deportivos, conciertos, en zonas arqueológicas, parques naturales, etcétera) y podrían emplear símbolos para facilitar el reconocimiento y sintetizar la información. Cabe usar también redes sociales, zonas de exhibición pública en lugares cerrados (p. ej. pantallas de televisión en un estadio deportivo), emisión de señal inalámbrica, luces intermitentes, indicadores acústicos y colores brillantes. Además, garantizar que el operador del dron tenga gran visibilidad facilita el ejercicio de los derechos de otras personas. El requisito de mostrar una marca de registro (similar a una matrícula de vehículo) solo es pertinente en la medida en que los drones sean visibles desde el suelo o si hay pérdida de control y los datos almacenados deben redirigirse al operador. Exigir la transmisión de una señal de marca de registro inalámbrica que pueda cotejarse con una base de datos en línea es otra solución interesante. No obstante, deben también tenerse en cuenta las preocupaciones relativas a la protección de datos y la seguridad de estos que plantea un sistema de registro[44].

---

[41] La propuesta anteriormente referida de la Comisión Europea para un reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos prevé la realización de una evaluación de impacto sobre la protección de datos en casos específicos (véase, en particular, el art. 33).

[42] El mecanismo de utilización de etiquetas que indiquen el consentimiento de los interesados al uso y la publicación de su imagen se describió en el proyecto Offlinetags (véase: http://offlinetags.net/en).

[43] De hecho, el GT 29 reconoce que el uso de los RPAS plantea el problema de cómo proporcionar información o hacer que el interesado consulte información sobre un dispositivo que a veces es tan invisible que su presencia o la recogida de datos pasan desapercibidos. Aunque informar al interesado que asiste a una actividad al aire libre sea fácilmente realizable mediante paneles de aviso sobre privacidad situados a la entrada de la zona controlada por RPAS, se plantea la cuestión de cómo proporcionar información sobre los RPAS que sobrevuelan el espacio público, sin limitaciones de alcance territorial claras.

[44] Por ejemplo, si una farmacia hace entregas regulares mediante dron a una propiedad de una persona, puede deducirse que el ocupante padece un problema médico grave. Exigir a una persona que presente planes de vuelo de drones o demuestre su capacidad de hacer búsquedas en el historial de vuelos de un usuario u organización de drones, incluyendo los sitios de despegue y aterrizaje, puede suscitar preocupaciones importantes sobre la protección de datos.

Adicionalmente, como práctica idónea, el GT 29 recomienda que los operadores de drones publiquen información en su sitio web o en plataformas específicas para informar constantemente sobre las diferentes operaciones que han tenido lugar y las previstas, mientras que, en las zonas remotas o donde sea improbable que las personas puedan acceder al sitio web, la información puede publicarse en periódicos, folletos o pósteres, o bien entregarse por correo postal[45].

En algunos Estados miembros, las AAC publican la lista de operadores a los que se permite hacer un uso profesional de los drones o la autorización concedida a cada operación. Ese tipo de listas es una opción aconsejable, ya que pueden facilitar el acceso a información sobre las operaciones de tratamiento de datos. Además, puesto que en muchos Estados miembros donde está regulado el uso de los drones, las operaciones con drones no están permitidas por diferentes motivos en algunas zonas, la publicación de mapas (que llevan a cabo las AAC y que los fabricantes pueden indicar, por ejemplo publicando un enlace a un recurso de información gestionado por las AAC) que muestran las zonas donde pueden usarse drones sería muy útil (por ejemplo, la publicación de este mapa ayudaría a las personas a identificar las zonas en las que pueden estar operando drones).

Este mismo enfoque de canales múltiples podría ser aconsejable en casos en los que los drones se utilicen para llevar a cabo vigilancia en grandes infraestructuras (por ejemplo, redes de ferrocarril o redes eléctricas). La información puede ofrecerse mediante señalizaciones y símbolos y, donde sea posible, sitios web. Tal información podría darse de forma genérica, explicando que la infraestructura está siendo supervisada, sin que sea necesario ofrecer detalles sobre los vuelos previstos o realizados, por ejemplo.

Por último, se ha sugerido por lo que respecta a las aplicaciones con drones que pueden cubrir zonas más extensas, donde la provisión de información a los interesados resulta más difícil o bastante imposible, la creación de un recurso de información nacional o transnacional (más fácil de encontrar que los sitios web de operadores individuales) para permitir a las personas identificar las misiones y operadores vinculados a drones concretos[46]. El GT 29 reconoce lo deseable de tal solución y pide a la Comisión Europea que haga uso de instrumentos de financiación para apoyar las investigaciones e inversiones a este respecto, sobre posibles placas de matrícula inteligentes para drones y similares.[47]

3.6 Seguridad del tratamiento de datos y cuestiones relacionadas, periodos de almacenamiento, comprobación previa

De acuerdo con el artículo 17 de la Directiva, los responsables del tratamiento y los encargados del mismo, donde sea aplicable, deben implementar medidas técnicas y organizativas apropiadas para proteger el tratamiento de datos personales frente a destrucción ilícita o pérdida accidental, alteración, así como revelación o acceso no autorizados. Esta disposición es aplicable también a los ataques electrónicos y los ciberataques (es decir, manipulación a distancia del dispositivo para tomar el control completo o parcial del mismo u obtener acceso a los sensores o a los datos almacenados).

[45] Por ejemplo, un agente inmobiliario que utilice un dron para hacer grabaciones de una propiedad en venta podría escribir a los vecinos por anticipado pero también visitar las propiedades vecinas el día de la grabación para alertarles de dicho tratamiento.

[46] Grupo de Trabajo sobre Protección de Datos en las Telecomunicaciones, Documento de trabajo sobre privacidad y vigilancia aérea, 54.ª reunión, Berlín, septiembre de 2013, publicado enwww.berlin-privacy-group.org.

[47] En determinados contextos muy sensibles, podría plantearse también la introducción de mecanismos de retroalimentación para verificar la realización de procedimientos específicos relacionados con la protección de datos. Por lo que se refiere a las acciones específicas previstas en los programas Horizon 2020 y COSME para apoyar el desarrollo del mercado de los RPAS, véase la comunicación de la Unión Europea «Una nueva era de la aviación. Abrir el mercado de la aviación al uso civil de sistemas de aeronaves pilotadas de forma remota de manera segura y sostenible», ibíd., acción 6. La tarea de mantener este recurso (que podría ser un sitio web específico donde se puedan rastrear los drones por adelantado, en el momento y con posterioridad, junto con un registro central accesible públicamente) se podría confiar, por ejemplo, a la EASA, a las autoridades de aviación nacionales o a las APD, y los legisladores podrían introducir también la obligación de informarles, no solo de los vuelos previstos, sino también del propósito del tratamiento de datos personales que tendrá lugar. A este respecto, debe recordarse que, en todo caso, en la mayoría de supuestos es necesario informar a las AAC de toda actividad con drones para obtener autorización. Véase, en este sentido, el párr. 3.8 del presente dictamen.

Esta protección también debe aplicarse a la fase de transmisión de datos personales desde el dron a la estación base. Se recomienda que los diseñadores de los drones y los equipos adaptados para montarse en los drones trabajen con expertos en seguridad apropiados para garantizar que se aborden adecuadamente las vulnerabilidades de seguridad.

Además, los datos personales procesados mediante drones no pueden almacenarse durante un periodo mayor del necesario para los fines del tratamiento[48]. Los datos que no estén vinculados a ninguna queja o problema deben borrarse o anonimizarse de inmediato.

Podría ser aconsejable incorporar horarios de almacenamiento y eliminación. Por consiguiente, los dispositivos que llevan los drones deben diseñarse de tal modo que permita establecer un periodo de almacenamiento definido para los datos personales recopilados y, en consecuencia, el borrado automático regular de aquellos datos personales que ya no sean necesarios de acuerdo con los horarios de eliminación.

En relación con todos estos aspectos, el GT 29 desea llamar la atención de los responsables del tratamiento al menos sobre lo siguiente:

- Debe permitirse a un número limitado de personas autorizadas, que se deberá especificar, la visión de las imágenes registradas o el acceso a las mismas
- Debe concederse el acceso limitado a las personas antes mencionadas en función de una necesidad de conocimiento puntual
- Almacenamiento y transmisión cifrados de la información donde sea necesario
- Registros de todos los casos de acceso y utilización del material grabado
- Periodos estrictos de almacenamiento de datos y borrado o anonimización automáticos una vez que haya expirado el periodo de almacenamiento de los datos
- Notificación de infracción de los datos a la APD (en la medida en que sea legalmente obligado)

Según las leyes de protección de datos nacionales pertinentes, podría haber medidas y disposiciones adicionales derivadas de la evaluación preliminar del tratamiento con arreglo al mecanismo de comprobación previa (véase el artículo 20 de la Directiva).

4. Papel de la cooperación entre diferentes actores e importancia de las herramientas autorreguladoras

La cooperación entre las APD y las AAC desempeña un importante papel a la hora de aumentar la concienciación entre los fabricantes, los operadores y los pilotos sobre las cuestiones de protección de datos ligadas al uso de los drones montados con equipos de detección. Para abordar esta cuestión se podrían usar cursos de formación, acontecimientos públicos y folletos comunes. Además, debe considerarse también si existen fases dentro del actual procedimiento aplicado por las ACC para conceder licencias a los pilotos de drones y certificar a los operadores de drones que pudieran ofrecer una buena oportunidad de abordar los aspectos de privacidad y protección de datos relacionados con el uso de drones.

En la mayoría de los casos, las AAC conceden certificaciones o autorizaciones muy específicas que regulan el uso de drones civiles: el área y la trayectoria de vuelo, el dispositivo y el operador y controlador con frecuencia se examinan en este contexto[49].

---

[48] Por ejemplo, las imágenes y vídeos captados por drones con el fin de asegurar el espacio abierto de un festival solo se conservarán durante el tiempo necesario para investigar posibles quejas o problemas relacionados con la seguridad.

[49] Véase a este respecto los resultados de una investigación realizada entre las AAC y publicada en Rachel L. Finn, David Wright y Anna Donovan (Trilateral Research & Consulting, LLP), Laura Jacques y Paul De Hert (Universidad Libre de Bruselas), *Privacy, data protection and ethical risks in civil RPAS operations*, página 145 y sig. y, para una descripción del actual marco regulatorio de los drones a escala europea y nacional, página 363 y sig.

En algunos países, el cumplimiento de los requisitos de protección de datos forma ya parte de un examen discrecional que llevan a cabo las autoridades aeronáuticas competentes al conceder permisos de operación de aeronaves[50]. Dado que este es el marco, informar a las AAC competentes de que se han tenido en cuenta todos los requisitos establecidos por la legislación de protección de datos, del tratamiento de datos personales previsto y de sus fines es una buena práctica que debe apoyarse, ya que podría también ayudar a llamar la atención de los operadores sobre los aspectos relacionados con la protección de datos antes de cualquier vuelo autorizado[51], y podría ayudar a elaborar una base de datos central de pública disposición en la que pudiera guardarse al menos la lista de operadores (incluyendo una descripción genérica de los fines para los que puedan procesarse los datos personales)[52]. Esto no significa que las AAC vayan a asumir la responsabilidad de comprobar que el operador de drones ha tomado las medidas apropiadas para cumplir con la legislación de protección de datos, pero es un control útil que forzará al operador de drones a tomar una decisión consciente relativa a las medidas que adoptará y si consideran estas suficientes.

Podría plantearse la promoción de códigos de conducta y esquemas de certificación para los fabricantes y operadores a fin de mejorar la concienciación de los operadores de drones civiles y su entendimiento de las cuestiones de protección de datos así como para ayudar a las APD a supervisar el cumplimiento. El importante papel que los códigos de conducta podrían tener en este marco es aún más concebible teniendo en cuenta que las APD no pueden evaluar o perseguir infracciones de privacidad de más envergadura cuando estas escapan a sus facultades legales, y en este sentido es cuando la responsabilidad de los operadores de drones puede resultar útil.

Por último, los distintivos de protección de la intimidad pueden desempeñar también un papel útil. Aunque estos esquemas no eximen a los responsables del tratamiento de conocer sus compromisos de protección de datos y protección de la intimidad, la participación de los operadores y fabricantes de drones en un enfoque de distintivos de protección de la intimidad con carácter general podría promoverse como un medio de favorecer la responsabilidad y el cumplimiento.

5. Indicaciones y recomendaciones finales

En vista de los riesgos y consecuencias potenciales que podría acarrear para la intimidad de las personas y las libertades civiles y políticas la apertura del mercado de la aviación a los drones, el GT 29 desea llamar la atención de los legisladores europeos y nacionales, los fabricantes de drones y equipos correspondientes, así como los operadores y usuarios de los drones sobre las siguientes indicaciones y recomendaciones, que pretenden ofrecer directrices añadidas a las ya contenidas en los dictámenes y documentos del GT 29 a los que hace referencia el presente dictamen.

5.1 Pasos que deben darse antes de manejar un dron:

1. Comprobar si la legislación nacional permite manejar drones y verificar la necesidad de una autorización específica de las AAC;
2. Aclarar las funciones de los diversos actores posibles: si el tratamiento no lo lleva cabo directamente el responsable, asegurarse de que esté regido por un contrato o un acto legal que vincule al encargado con el responsable y que el encargado actúe solo siguiendo instrucciones del responsable;

---

[50] Ibíd. Por ejemplo, el examen para obtener la licencia al que debe someterse un piloto de RPAS podría incluir algunos conocimientos previos de la legislación sobre privacidad y protección de datos para asegurarse de que los pilotos conozcan las obligaciones legales en caso de tratamiento de datos personales.

[51] Por ejemplo, en Alemania, la normativa de tráfico aéreo (Luftverkehrs-Ordnung, la LuftVO) se modificó en 2012 para incluir el cumplimiento de los requisitos sobre protección de datos como parte de un examen discrecional pertinente por parte de las autoridades aeronáuticas competentes de los estados federados al conceder permisos para operar aeronaves.
De modo similar, el reglamento sobre vehículos aéreos pilotados de forma remota adoptado en Italia el 16 de diciembre de 2013 estipula que, «cuando las operaciones llevadas a cabo por un RPAS puedan acarrear el tratamiento de datos personales, este hecho deberá comunicarse en la documentación presentada para la concesión de la autorización pertinente» (artículo 22).

[52] Esto puede también responder a las preocupaciones de seguridad, ya que hay noticias recientes de drones sobrevolando ilegalmente edificios estratégicos de zonas urbanas sin posibilidad alguna de identificar a las personas que operaban los drones.

3. Evaluar el impacto sobre la protección de datos teniendo en cuenta el propósito de las operaciones y el tipo de drones (dimensión, visibilidad, etcétera) y las combinaciones específicas de tecnología de detección a bordo de los mismos; determinar los fundamentos jurídicos más apropiados (consentimiento de los interesados, ejecución de un contrato, obligación legal, interés legítimo, etcétera) y la posible necesidad de notificar o consultar a las APD competentes según la legislación de protección de datos nacional;
4. Elegir la tecnología a bordo más proporcionada y adoptar todas las medidas adecuadas de privacidad por defecto: establecer servicios y productos de tal modo que se evite la recopilación y el tratamiento posterior de datos personales innecesarios;
5. Encontrar el modo más apropiado de informar a quienes van a verse afectados por el tratamiento de datos: informar mediante señalizaciones u hojas informativas en caso de operación visual en un área especificada; en caso de alguna actividad, informar al público mediante las redes sociales, periódicos, folletos o pósteres; ofrecer información clara siempre sobre el sitio web correspondiente: el aviso debe contener una indicación clara del responsable del tratamiento y los fines del mismo y debe ofrecer a los interesados indicaciones claras y específicas para ejercer el derecho de acceso a los registros visuales y no visuales que les afecten;
6. Tomar todas las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado a los riesgos que supone el tratamiento y la naturaleza de los datos que deben protegerse, en particular para prevenir cualquier tratamiento no autorizado también durante la fase de «transmisión»;
7. Eliminar o anonimizar cualquier dato personal innecesario lo antes posible tras la recopilación.

5.2 Recomendaciones a los responsables normativos y los reguladores del sector

La apertura del mercado aeronáutico al uso civil de los drones debe ir paralelo a:

1. La promoción, en el ámbito europeo y nacional, de un marco que garantice no solo la seguridad de los vuelos sino también el respeto de todos los derechos fundamentales. A este respecto, el GT 29 reclama la implicación de todas las partes interesadas relevantes en el debate relativo a la integración de los drones en el espacio aéreo civil;
2. La armonización y modernización de las políticas de los Estados miembros que sean pertinentes en relación con los drones, incluyendo la cuestión del derecho aplicable a las operaciones con drones transfronterizas;
3. La introducción, como parte del marco mencionado, de normas específicas que garanticen un uso responsable de los drones, que deben incluir necesariamente el respeto de las zonas privadas (como jardines, patios, terrazas, entre otros); con ese fin, debe plantearse la introducción, cuando sea necesario, de perímetros virtuales (o zonas de exclusión de vuelo). Además, puesto que el uso de los drones puede estar limitado a zonas muy específicas en muchos Estados miembros, la publicación de mapas por parte de la AAC ayudaría a los usuarios a saber dónde está permitido el uso de drones (considerando que se respeten los demás principios);
4. La introducción de una obligación, a escala europea o nacional, para los fabricantes de comercializar los drones más pequeños solo si van acompañados de suficiente información (por ejemplo dentro de las instrucciones de manejo) relativa a la intrusividad potencial de estas tecnologías y recordando la necesidad de respetar la legislación europea y nacional así como los reglamentos que protegen la intimidad, los datos personales y otros derechos fundamentales;
5. El desarrollo y la introducción por parte de los responsables normativos competentes, a

escala europea y nacional, en consulta estrecha con los representantes del sector, de criterios de evaluación de impacto en la protección de datos que el sector y los operadores puedan aplicar fácilmente;

6. La introducción de aspectos de protección de datos entre los elementos clave de las disposiciones nacionales que regulan el uso comercial de los drones (en relación con la cualificación y la formación de los pilotos, entre los requisitos de aeronavegabilidad y certificación, al emitir o revocar licencias de operación y permisos de trabajo aéreo, etcétera); en particular, las declaraciones de haber tenido en cuenta los requisitos de protección de datos podrían formar parte de las condiciones de concesión de un permiso;
7. La promoción de certificaciones de protección de datos a fin de mejorar la concienciación de los operadores de drones civiles y su entendimiento de las cuestiones de protección de datos así como para supervisar el cumplimiento;
8. Además, el GT 29 recomienda que la Comisión Europea haga uso de programas de financiación para apoyar las investigaciones e inversiones en nuevas tecnologías cuyo fin sea incrementar la transparencia (nuevas tecnologías para informar al público en general de los vuelos de drones y sus fines así como el ejercicio de sus derechos de acceso) que incluya, por ejemplo, placas de matrículas inteligentes o un sitio web que publique información en tiempo real sobre todas las operaciones con drones.

5.3 Recomendaciones a los fabricantes y operadores

1. Incorporar opciones de diseño respetuosas de la privacidad y funciones predeterminadas como parte de un enfoque de privacidad por diseño;
2. Hacer partícipe a un delegado de la protección de datos (donde se disponga del mismo) en el diseño y la implementación de políticas relativas al uso de los drones;
3. Promover y adoptar códigos de conducta que puedan ayudar al sector y a las diferentes categorías de operadores a prevenir las infracciones y aumentar la aceptabilidad social de los drones; tales códigos deberían contener sanciones en caso de que los firmantes incumplan el código;
4. Hacer que los drones sean lo más visibles e identificables posible (mediante la emisión de una señal inalámbrica, luces parpadeantes, indicadores acústicos o colores brillantes);
5. Cuando se hallen en la línea de visión, hacer que el operador sea visible e identificable con claridad mediante señalización como la persona responsable del dron;
6. Cuando se planifique y se opere un vuelo, incluso si se permite operar el dron sobre zonas pobladas, evitar lo máximo posible volar por encima o cerca de zonas y edificios privados.

5.4 Recomendaciones para el uso de los datos personales recopilados mediante aviones no tripulados (drones) con fines policiales

De modo similar al uso de los drones con fines comerciales, el uso de los datos personales recabados mediante drones por la policía y otras autoridades de orden público debe:

1. Cumplir con los principios de necesidad, proporcionalidad, limitación de fines, minimización de los datos y privacidad por diseño; debe establecerse un periodo de conservación estricto y justificado;
2. Hay que respetar el principio de transparencia: debe establecerse por ley que el tratamiento de datos llevado a cabo mediante drones sea transparente y previsible para los interesados; estos, en la medida de lo posible, deben ser informados del tratamiento y de sus derechos correspondientes;
3. El tratamiento de datos con fines policiales llevado a cabo mediante drones no debe permitir el seguimiento constante de las personas o, a lo sumo, cuando se determine que el seguimiento es estrictamente necesario, este deberá estar limitado a investigaciones

policiales con garantías. Los equipos técnicos y de detección usados deben ser acordes con el propósito del tratamiento;

4. La prohibición de ejecución automatizada de decisiones es aplicable también a estos usos. Los datos procesados mediante drones deben someterse al examen minucioso posterior de un operador humano antes de tomar cualquier decisión que afecte negativamente a una persona;
5. En general, los tribunales deben ser capaces de revisar el uso de los drones con fines de información y policiales con arreglo a las prácticas nacionales;
6. Se llevará a cabo un examen regular de la necesidad de procesar datos personales mediante drones y de la conformidad de este uso con los marcos jurídicos en evolución;
7. Además, el uso de drones con fines policiales, incluso en caso de investigaciones con garantías –como puede ser una vigilancia específica–, requeriría un régimen de autorización superior en la jerarquía. En función de la legislación nacional, los datos personales recabados mediante drones para estos tipos de investigaciones deben incorporarse en los ficheros administrativos que pueden usarse judicialmente.