Los drones y los derechos fundamentales en la UE

*Drones and fundamental rights in the EU**

Clara GONZÁLEZ PUENTE
Capello & Focanti Internacional
clargonz93@hotmail.com

Fernando GONZÁLEZ BOTIJA
Universidad Complutense de Madrid (España)
dp143@ucm.es

Recepción: Febrero 2018
Aceptación: Abril 2018

RESUMEN

A la luz de la progresiva integración de los drones en el espacio aéreo civil europeo y de la aparición de numerosos usos de los drones (que van desde el ocio a los servicios, la fotografía, la logística y la vigilancia de las infraestructuras), es necesario centrarse en los desafíos que plantea el despliegue a gran escala de la tecnología de drones y sensores. Esto podría interferir en la privacidad de las personas y en sus libertades civiles y políticas. Por tanto, en el nivel europeo hay que evaluar las medidas necesarias para garantizar el respeto de los derechos fundamentales y la protección de datos.

Palabras clave: Dron, Vehículos aéreos no tripulados, Derechos fundamentales, Protección de datos.

Clasificación JEL: K32.

* El presente trabajo se ha realizado en el marco del Proyecto I+D, Referencia DER2017-87981-P, titulado "El régimen jurídico-público de los drones", y del que son I.P.s los profesores Juan Ramón Fernández Torres y Fernando González Botija.

ABSTRACT

In light of the progressive integration of drones into the European civil airspace and the emergence of numerous applications of drones (ranging from leisure, services, photography, logistics, surveillance of infrastructures) there is a real need to focus on the challenges that a large-scale deployment of drone and sensor technology could bring about for individuals' privacy and civil and political liberties and to assess at European level the measures necessary to ensure the respect for fundamental rights and data protection.

Key words: Drone, Unmanned Aerial Vehicle, Fundamental rights, Data protection.

JEL classification: K32.

1. INTRODUCCIÓN

Los comúnmente llamados "drones", son vehículos aéreos no tripulados - *UAV (Unmanned Aerial Vehicle)* en inglés – es decir, aeronaves que vuelan sin tripulación. Esta tecnología puntera ha llegado hace poco al uso civil, pero lleva años siendo utilizada en aplicaciones militares, como vehículo de inspección, vigilancia e incluso ataque. Los drones son capaces de mantener de manera autónoma el vuelo, el cual puede ser controlado remotamente o previamente establecido en un plan de vuelo pre programado[1]. La principal controversia de este tipo de tecnología autónoma, que no necesita del ser humano para realizar sus funciones, es precisamente la posibilidad de que estos artilugios no tripulados puedan causar daños colaterales a objetivos erróneamente identificados. Es por ello que su aplicación militar es tan controvertida, aunque también se utilicen en labores más pacíficas como vamos a ver.

Este tipo de vehículos aéreos no pilotados surgieron en la década de los 70 y fueron desarrollados por las Fuerzas Aéreas de Israel. Su uso comenzó a implantarse a partir de los años 90 en el ámbito militar, como herramienta principal en las misiones de reconocimiento. Tras los ataques terroristas de Nueva York y Washington del 11 de septiembre de 2001, los Estados Unidos comenzaron a utilizar los primeros drones armados en Yemen en 2002, transformando el propósito inicial de vigilancia y control con que habían sido ideados estos elementos, para convertirlos en máquinas capaces de realizar ataques en zonas remotas, con solo pulsar un botón. Los drones incorporan en su sistema un conjunto de cámaras de alta resolución e infrarrojos, capaces de transmitir imágenes en tiempo real y de captar e identificar un objetivo en tierra desde el aire.

Desde su creación, el uso de drones se ha generalizado. Los drones actuales no solo son capaces de mantener el vuelo durante más tiempo y a mayor distancia del centro de control, sino que han incorporado también sistemas de aterrizaje automático e incluso están siendo programados para ser capaces de tomar decisiones autónomas en momentos críticos. Este hecho ha traído consigo situaciones como la muerte de cientos de civiles, entre ellos niños, causadas por el error de estas máquinas en la detección de objetivos en las zonas de conflicto. Ante estas circunstancias, se plantea un debate ético y moral sobre el uso de drones armados autónomos en estas zonas en guerra.

Naciones Unidas lleva años pidiendo a la comunidad internacional que cese en el empleo de este tipo de vehículos aéreos armados hasta que exista una mayor base legal para su uso y, en todo caso, se respeten las leyes internacionales existentes y permitan que se lleven a cabo las investigaciones precisas en los casos en que se hayan reportado ataques ilícitos sobre población civil.

El uso de estos vehículos no tripulados se ha extendido tanto en los últimos años que su utilización hoy en día es generalizada, tanto en su aplicación militar y de seguridad nacional, como en el uso privado particular. Tradicionalmente concebidos como un medio para realizar acciones de vigilancia en zonas de conflicto, también han sido utilizadas para otros usos. El problema de los drones no viene dado únicamente por su uso gubernamental; cada vez hay más y más personas que utilizan este tipo de vehículos de modo particular, ya sea para el ejercicio de su profesión como para el uso recreativo. En sus nuevas versiones los drones no son solamente armas militares, sino que se utilizan para fines más nobles y que innegablemente interfieren menos con los derechos humanos. Hoy en día los drones se utilizan en operaciones de rescate y salvamento (permitiendo el acceso a zonas aisladas o afectadas por desastres naturales lucha contra incendios, etc), en eventos deportivos o grandes aglomeraciones de personas, para la vigilancia del tráfico o infraestructuras o la exploración de territorios salvajes y el estudio de sus especies vegetales y animales. Son capaces de transmitir, no solo imágenes, sino datos meteorológicos, niveles de radiación o de concentración de gas etc., y todo a tiempo real. Capaces de llegar a zonas no accesibles para el hombre o para otro tipo de vehículo tripulado, sus aplicaciones positivas son infinititas y suponen un menor coste moral y ético[2].

En la UE a fecha de hoy existe un marco regulatorio en el nivel comunitario contenido en el Reglamento 216/2008 sobre Normas Comunes en el Campo de la Aviación Civil[3]. La competencia europea se ciñe a los drones de uso particular y de más de 150kg. Los de peso inferior no entrarían dentro de lo que la Agencia Europea de Seguridad Aérea (en adelante, EASA) considera un UAV por lo que estarían regulados por normas nacionales como hacen varios Estados pertenecientes a la UE, como República Checa, Dinamarca, Suecia, Alemania, Reino Unido o España. Hay que advertir que está en marcha una modificación importante de este marco legal. El fin que persigue la UE es precisamente seguir el ejemplo de estos Estados miembros para crear una norma europea que unifique el uso de drones – independientemente de su tamaño o peso - en toda la Unión. En agosto de 2016 la EASA ha presentado una primera propuesta regulatoria a la Comisión[4], después de que en 2015 elaborara una Opinión Técnica[5], en la que clasificaba los drones en tres niveles de riesgo - bajo, medio y alto – según las características del vehículo y el uso que pretendía hacerse de él. En este texto, la EASA reflexiona sobre la importancia de crear una norma que, junto con las leyes nacionales, garantice el uso responsable de los UAV. Representa los puntos de vista de la Agencia, pero no constituye ningún compromiso formal por parte suya ni de la Comisión Europea.

Dentro de este deseo de reforma las instituciones comunitarias han sido conscientes de que no se puede obviar un tema de primera magnitud al tratar esta cuestión: el problema que plantea con relación a la protección de los derechos fundamentales. Aunque existe un reconocimiento unánime de los beneficios sociales y económicos del uso civil de drones y su potencial para impulsar el crecimiento y el empleo, no se deben igualmente olvidar

todas las amenazas y riesgos que para la protección de datos y la privacidad de los ciudadanos pueden resultar de un despliegue a gran escala de la tecnología de drones. Por ello es necesario evaluar las medidas necesarias para garantizar el respeto de todos los derechos fundamentales en juego. La Unión se basa 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. Por tanto, es necesario equilibrar todos los derechos e intereses en juego, que los responsables de la formulación de políticas no pueden ignorar para garantizar que Europa pueda estar a la vanguardia en este nuevo sector. Así se ha realizado una y otra vez al tratar el tema de los drones.

La necesidad de garantizar esa protección ya aparece en abril de 2014 en la Comunicación de la Comisión dirigida al Parlamento europeo y al Consejo titulada "Una nueva era de la aviación: Abrir el mercado de la aviación al uso civil de sistemas de aeronaves pilotadas por control remoto de manera segura y sostenible"[6]. En este documento se advierte que los riesgos identificados con mayor frecuencia están relacionados con el uso de equipos de vigilancia instalados en los drones y la recopilación de datos. Por eso la Comisión (como "acción 4") proponía que en la apertura del mercado de la aviación a los drones se evaluaría la forma de garantizar la conformidad de sus aplicaciones con las normas sobre derechos fundamentales. En concreto se insistía en que las operaciones de drones debían respetar la Carta de los Derechos Fundamentales de la Unión Europea[7]. Según el ejecutivo comunitario, el desarrollo de una amplia gama de aplicaciones civiles potenciales de los drones exigía asimismo garantizar que ninguna pudiese llegar a suscitar problemas de orden ético o representar una amenaza para la privacidad (derecho a la intimidad personal y familiar) o integridad física de los ciudadanos y un atentado contra la protección de datos privados en particular en los ámbitos de la vigilancia, el seguimiento, la cartografía o los registros de vídeo. Estas ideas de la Comunicación de 2014 fueron asumidas en 2015 en la Declaración de Riga[8]. Se llamaba la atención sobre el hecho de que la aceptación del público era clave para garantizar el crecimiento de los servicios de drones.

No es posible, por lo tanto, que no exista formalmente una normativa que limite en cierto modo el uso de estos aparatos o que se pronuncie al menos sobre las responsabilidades en que pueden incurrir quienes hagan un uso indebido de las imágenes captadas por los mismos.

2. ¿POR QUÉ LOS DRONES SON UNA AMENAZA PARA LOS DERECHOS FUNDAMENTALES Y CUÁLES DE ELLOS SE VEN AFECTADOS?

En los informes del Grupo de Trabajo del artículo 29[9] se aclara que, en términos generales, los drones son vehículos aéreos que pueden pertenecer a diferentes categorías con una amplia variedad de especificaciones, características y capacidades. Igualmente se pueden diseñar para admitir una variedad de cargas útiles que varían en tamaño y capacidad técnica[10]. Sin embargo, en cualquier caso, deja claro que lo relevante, desde el

punto de vista de la protección de los derechos fundamentales, no es el uso del dron per se, sino el equipo de captación de datos que puede existir a bordo del dron y su posterior tratamiento[11]. En la mayoría de sus usos los drones tratan datos (incluso más que los aviones tradicionales[12] y las cámaras de circuito cerrado de televisión –en lo sucesivo CCTV-[13]), lo que desencadena la aplicación del marco legal de protección de datos. La tecnología incorporada ofrecerá así la posibilidad de recopilar, registrar, organizar, almacenar, utilizar y combinar datos que permitan a los operadores identificar personas directa o indirectamente. Esta identificación podría ser realizada por un operador humano, seleccionando automáticamente la imagen tomada del programa de reconocimiento facial de una base de datos existente y usándolo para identificar a la persona, usando RFID[14] en los pasaportes, etc. Los drones se pueden usar con tecnología que mejora la visión humana y captura detalles que los humanos no pueden ver. Tirando de este hilo el Supervisor Europeo de Protección de Datos (en lo sucesivo SEPD), subraya que el problema no es lo que estos aparatos son capaces de captar durante su vuelo, sino el uso que posteriormente se dé a esa información[15]. El material obtenido por las cámaras integradas en los drones es susceptible de utilizarse en fines comerciales, profesionales, privados e incluso en investigaciones policiales o de los servicios de inteligencia gubernamentales. Tampoco hay que olvidar que su bajo costo y sus características técnicas, como vamos a ver, los convierten en herramientas únicas, muy efectivas y discretas para misiones de vigilancia y control.

Por tanto, dentro de esta amplia variedad de usos, los riesgos para los derechos humanos dimanan de varios aspectos técnicos que poseen estos aparatos. Hay que tener en cuenta que los sistemas de aeronaves pilotadas a distancia tienen el mismo potencial de interferir gravemente con los derechos a la vida privada y familiar y a la protección de datos que las tecnologías en línea consideradas por el Tribunal de Justicia de la Unión Europea en los asuntos Derechos Digitales Irlanda c. Seitlinger[16] y Google España[17], decisiones que deben ser tenidas en cuenta. No hay que olvidar su movilidad (velocidad y cambios de altitud), resistencia y la posibilidad de realizar vuelos silenciosos.

Quizás el más relevante aspecto desde el punto de vista técnico sobre el que hay que hacer hincapié, reside en el hecho de que el dron puede incorporar a bordo una cámara con software especializado con una resolución muy alta, unos equipos, micrófonos y sensores de gran potencia muy sofisticados (térmicos, biométricos)[18] con los que capta un conjunto inmenso de datos[19]: imágenes (de personas, casas, vehículos, matrículas, etc.), sonidos (sistemas de grabación de audio), datos de geolocalización o GPS (que procesan la ubicación de la persona filmada) o cualquier otra señal electromagnética relacionada con una persona física identificada o identificable. Además, cuando se combinan con otras tecnologías, los drones pueden convertirse en herramientas de vigilancia extremadamente poderosas. Ello debido a que pueden llevar una multitud de sensores, realizar una vigilancia sistemática (abierta y encubierta) de un individuo o grupos (en caso de manifestaciones, por ejemplo) y ser extremadamente versátiles (pueden ir a casi cualquier

lugar), ofreciendo un nivel superior de vigilancia. Por ejemplo, pueden volar sobre jardines cerrados, seguir a las personas en las calles, detectar y contar cuántas personas hay en un edificio o en una habitación en particular. La tecnología que pueden transportar, el hecho de que las baterías tienen una vida útil cada vez mayor y el que puedan ser grandes y visibles o pequeños y casi invisibles (subrepticio, clandestino) ayudan a hacerlos potencialmente cada vez más intrusivos en lo que respecta la privacidad de los ciudadanos[20].

Hay que considerar igualmente que estos aparatos están dotados de una gran destreza que facilita aún más su capacidad para lograr puntos de observación únicos, por ejemplo, para evitar obstáculos y no verse limitado por barreras, muros o vallas. Por lo tanto, pueden recoger con mayor facilidad en instalaciones privadas una gran variedad de información de diversas fuentes. Dependiendo de las tecnologías a bordo, los datos podrían recopilarse sin necesidad de una línea de visión directa (es decir, a través de techos, escombros o nubes), durante largos períodos de tiempo y en grandes áreas sin interrupción.

Tampoco hay que olvidar que, dada su flexibilidad y discreción, los interesados afectados encuentran grandes dificultades para identificar los drones, pues estos dispositivos pueden ser difíciles de ver desde el terreno. En cualquier caso, incluso si las personas son conscientes de que hay un avión no tripulado en la zona, es difícil que sepan qué equipo de tratamiento de datos lleva a bordo y para qué fin están siendo recogidos y por quién. Esto dará lugar a una mayor sensación de estar bajo vigilancia, con el consecuente recorte en el ejercicio legítimo de las libertades y los derechos civiles[21]. Por lo tanto, existe un alto riesgo de que el tratamiento de datos personales por los drones se oculte e interfiera grandemente en la esfera más íntima de las personas. Al mismo tiempo, existe un riesgo innegablemente más alto de cambio o extensión del uso inicialmente previsto para dirigirlo a un fin incompatible.

Todo esto que acabamos de señalar conduce a que generan un alto riesgo de captar datos de manera masiva lo que, dada su naturaleza peculiar y su uso cada vez más habitual, supera con mucho la efectividad y capacidad de las cámaras CCTV fijas. Es decir, los drones destinados a la vigilancia, tanto pública como privada, pueden almacenar y procesar datos e imágenes de gran cantidad de población, que estaría sometida a una vigilancia continuada sin saberlo y sin ser consciente de ello. No hay que olvidar que pueden sobrevolar zonas habitadas densamente pobladas. También se debe considerar la posibilidad de interconectar una serie de drones con el fin de llevar a cabo la vigilancia en una gran área. La posibilidad de organizar "enjambres" de drones, con canales de comunicación en tiempo real entre ellos, desencadenaría aún mayores riesgos para la protección de datos, ya que podrían permitir fácilmente la vigilancia coordinada, es decir, el seguimiento de los movimientos de personas o vehículos en grandes zonas.

Finalmente, no hay que olvidar que el tipo de dron más básico que consta únicamente de componentes vitales (estructura, motor, rotor, batería, controlador de vuelo) puede no

estar tratando datos personales, pero aún puede causar molestias y perturbaciones sociales.

A la vista de este gran potencial de invasión tecnológica sobre la esfera individual no es de extrañar que sean muchos los derechos afectados. Es pues el momento de analizar los derechos fundamentales que se ponen en juego con el uso de estos vehículos aéreos. Hay que advertir que la integración de los drones en el mercado de la aviación europea y sus diferentes fines civiles (incluido el uso para objetivos legales), plantean desafíos específicos que deben superarse para respetar los derechos y principios consagrados en la Carta de los Derechos Fundamentales de la UE. Con este panorama se puede adivinar claramente una más que posible afectación del derecho a la vida privada y familiar (artículo 7 de la Carta de los Derechos Fundamentales de la Unión Europea y artículo 8 del Convenio del Consejo de Europa sobre el Derechos humanos)[22] y a la protección de los datos personales (artículo 8 de la Carta y artículo 16 del Tratado de Funcionamiento de la UE (en lo sucesivo, "el TFUE"). Con todo, no hay que descartar problemas relacionados con otras libertades y derechos conectados de un modo u otro a resultas de todo lo que se deriva del uso de estos aparatos (por ejemplo, libertades de expresión e información, derecho de reunión, derecho a la vida, a la integridad física y a la seguridad privada ante posibles daños sobre personas y bienes causados por los drones por accidente)[23]. Además, en la Declaración de Riga se recordaba que los drones podían causar molestias y externalidades negativas, como el ruido, afectando por tanto al medio ambiente. Estas molestias debían abordarse, posiblemente en el nivel local, para mantener la aceptación del público. También se apuntaba, como ya sabemos, que los drones planteaban posibles riesgos de seguridad pública. El diseño de los drones podía y debía tener en cuenta esos riesgos mediante el uso de métodos como la defensa cibernética o la georreferenciación. Sin embargo, se advertía que el uso malicioso de los drones no podía evitarse por completo mediante restricciones de diseño o de funcionamiento. Era, pues, tarea de los sistemas nacionales de policía y justicia abordar estos riesgos[24].

Para concluir este punto, nunca se debe olvidar que la percepción de los drones por los individuos está inextricablemente ligada a su sostenibilidad social. Desde el plano institucional se desea generar un debate público creando conciencia sobre las implicaciones de la utilización de los drones en materia de privacidad. A este respecto, la aplicación efectiva de la ley de protección de datos y del resto de la legislación sobre derechos humanos puede contribuir a la aceptación de los drones y a mejorar su mercado y su desarrollo industrial. La Comisión en su Comunicación de 2014 advertía que tenía previsto consultar a los expertos y a las partes interesadas pertinentes y abordar las medidas necesarias en su ámbito de competencia para proteger los derechos fundamentales, inclusive mediante acciones de concienciación, así como para fomentar la adopción de medidas por las autoridades nacionales en su ámbito de su competencia. El ejecutivo comunitario tenía claro que el cumplimiento de los requisitos de protección de datos impediría que sus capacidades "representasen una amenaza para la privacidad de

los ciudadanos". En la misma dirección el SEPD, respondiendo a una consulta de la Comisión, redunda en la idea de que, junto con otros requisitos (incluidas las normas de seguridad aérea, certificación / homologación, salud, etc.), el respeto de los requisitos de protección de datos y el derecho a la vida privada y familiar mejorará el desarrollo del mercado de drones en la UE de conformidad con los derechos fundamentales de las personas involucradas. De hecho, solo los drones que garanticen una adecuada protección de datos y de la privacidad en su diseño tendrán una buena aceptación social en general, es decir, no solo por las autoridades de protección de datos, las organizaciones y asociaciones de derechos fundamentales sin fines de lucro sino también por el público en general. Por ello el SEPD recibió con satisfacción que la Comunicación no solo subrayara los beneficios sociales y económicos esperados, sino que también identificara la privacidad, la protección de datos y la seguridad como elementos clave para garantizar la difusión del uso los drones[25]. Se tiene claro que el objetivo es garantizar que la legislación sobre el tema tenga plenamente en cuenta la necesidad de concienciar al público en general (fabricantes, controladores, encargados de tratamiento, usuarios, etc) en este sentido. El SEPD saluda las iniciativas y los proyectos de sensibilización que deberían acompañar a la introducción de los drones en el mercado civil de la UE. A este respecto subraya el trabajo que ya están realizando algunas autoridades nacionales de protección de datos sobre el impacto de los drones en el derecho al respeto de la privacidad y la protección de datos[26]. Por consiguiente, los Estados miembros y las instituciones de la UE tienen la obligación positiva de asegurar que, ya sea con fines comerciales o profesionales, policiales, de inteligencia o privados, los drones respeten los derechos esenciales de los ciudadanos.

3. EL ESPECIAL RESPETO A LA PROTECCION DE DATOS

Debemos dedicar un apartado especial al tema de la protección de datos porque el uso de los drones plantea una problemática muy relevante en este terreno ya que su utilización implica captar imágenes de personas físicas identificadas o identificables[27].

3.1 Introducción: el respeto a la legalidad

Desde la UE se ha insistido en la idea de que el uso de drones y el tratamiento de las imágenes y otros datos obtenidos mediante su uso, por parte de personas privadas, de las autoridades de un Estado Miembro, de las agencias de inteligencia o de cualquier otro organismo gubernamental o supranacional[28], debe ser conforme con el principio de legalidad[29]. Es decir, se debe cumplir con la legislación aplicable en general. Esto significa que no sólo hay que respetar la normativa de protección de datos, sino también la legislación nacional que salvaguarda los derechos personales, la imagen, la vida familiar y la esfera privada. El tratamiento de los datos personales debe ser legal en todos los aspectos, lo cual abarca otras reglas relevantes en áreas tales como el derecho civil o penal, la propiedad intelectual, el derecho aeronáutico o el ambiental. En los Estados

miembros donde la operación de drones viole las normas de aviación nacionales, se considerará que el tratamiento de los datos personales recopilados no cumple con el principio de legalidad. Todo ello, evidentemente, bajo el control judicial.

Hay que verificar si la ley nacional permite operar drones y verificar la necesidad de una autorización específica de las autoridades competentes. Hay que aclarar las funciones de los posibles actores que intervienen en cada operación. En la medida en que el tratamiento no sea realizado directamente por el controlador del aparato hay que asegurarse de que el tratamiento se rige por un contrato o acto legal que vincule al encargado del tratamiento con el controlador y que aquél actúe únicamente siguiendo instrucciones de éste.

Ya más en concreto, obviamente, los operadores de drones tendrán que cumplir las disposiciones aplicables en materia de protección de datos[30], en particular el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)[31]. Tampoco hay que olvidar que al ser utilizados por los proveedores de servicios de comunicaciones electrónicas disponibles al público (por ejemplo, para ampliar el alcance de tales servicios), habrá que tener en cuenta la Directiva 2002/58/CE, modificada por la Directiva 2009/136 /CE. Así mismo, los datos tratados posteriormente para fines comerciales, profesionales o administrativos deberán cumplir escrupulosamente con las normas nacionales[32] que aplican esta normativa comunitaria.

Hay que advertir que el 20 de mayo de 2014, el Grupo Europeo de Ética en Ciencia y Nuevas Tecnologías (GEE) emitió un dictamen sobre Ética de las Tecnologías de Seguridad y Vigilancia (n° 28) que abordó el uso de drones para misiones de vigilancia[33]. Al año siguiente, el 16 de junio de 2015, el Grupo de Trabajo del artículo 29 elaboró el denominado "Informe 01/2015 sobre privacidad y protección de datos relacionados con la utilización de Drones"[34]. Debido a las peculiaridades y riesgos antes mencionados de las aplicaciones de aviones no tripulados, el citado Grupo consideró importante proporcionar una guía específica sobre cómo cumplir con las normas de protección de datos en este contexto. También hay que tener en cuenta el estudio realizado por el Comité de Libertades Civiles, Justicia y Asuntos de Interior (*Committee on Civil Liberties, Justice and Home Affairs* o LIBE, en inglés) del Parlamento Europeo, sobre las consecuencias del uso civil de drones en los derechos a la vida privada y la protección de datos. Para su elaboración el LIBE se sirvió principalmente de las opiniones del Grupo de Trabajo del artículo 29 y del dictamen arriba citado del SEPD. En este informe se reflexiona en torno a la posibilidad de que el uso civil de drones provoque una interferencia grave en la vida privada de los ciudadanos[35].

En las siguientes líneas vamos a describir sintetizado el contenido de estos documentos.

3.2 Aplicación de exenciones o excepciones

En el Informe del Grupo de Trabajo del artículo 29 se advierte que algunos casos de tratamiento de datos personales derivados del uso de drones para operaciones civiles pueden quedar fuera del alcance de las directrices generales a la luz de exenciones o excepciones que, de acuerdo con la, entonces en vigor Directiva, los Estados miembros pueden establecer[36].

De conformidad con el artículo 2.2 c) del Reglamento 2016/679, el tratamiento de datos personales por una persona física en el ejercicio de una actividad puramente personal o doméstica quedará fuera del ámbito de análisis.

Sin embargo, al ser una excepción debe interpretarse de manera restrictiva. Según lo considerado por el TJUE, la llamada "exención de hogar" debe interpretarse como referida únicamente a actividades que se llevan a cabo en el curso de la vida privada o familiar de los individuos, o en su faceta de aficionados. Esta excepción de hogar podría ser relevante para algunos usos limitados de los drones. Hay que tener en cuenta que el hecho de que el fin original sea en principio doméstico no significa que no se haya de respetar la intimidad de otras personas si al final se demuestra que se ve afectada. Por eso, por ejemplo, se advierte que claramente no es el caso del tratamiento de los datos personales que consisten en su publicación en Internet para que sean accesibles a un número indefinido de personas. Es decir, el tratamiento de datos personales a través de drones realizado por usuarios privados no estaría dentro de la excepción de hogar en los casos en que el uso del dron esté destinado a compartir o incluso publicar las capturas / imágenes de video / sonido resultantes o cualquier información que permita la identificación directa o indirecta de un individuo en Internet y, en consecuencia, a un número indefinido de personas (por ejemplo, a través de una red social). Además, si las operaciones de un dron y su equipo a bordo incorporan un sistema de videovigilancia, no puede considerarse como una actividad puramente "personal o doméstica" en la medida en que implica la grabación constante y el almacenamiento de datos personales y cubre, "incluso parcialmente, un espacio público y por lo tanto, se dirige hacia afuera desde el entorno privado de la persona que procesa los datos de esa manera"[37].

La aplicación de estos criterios a los drones puede llevar en muchas ocasiones a concluir que estas excepciones difícilmente se podrían aplicar y que los usos privados pueden llegar a estar afectados por el actual Reglamento. Como se afirma en el documento citado, "ninguno de estos criterios es, en sí mismo, necesariamente determinante. Sin embargo, una combinación de estos factores se utilizará para determinar si el tratamiento realizado por un particular entra o no en el ámbito del ámbito personal o doméstico. Para este fin, uno debe determinar: 1º) si los datos personales se difunden a un número indefinido de personas, en lugar de a una comunidad limitada de amigos, familiares o conocidos, 2º) si los datos personales se refieren a individuos que no tienen relación personal o doméstica

con la persona que los publica, 3º) si la escala y la frecuencia del tratamiento de los datos personales sugieren una actividad profesional o a tiempo completo, 4º) si hay evidencia de que existe un grupo de individuos que actúan juntos de manera colectiva y organizada, 5º) si existe un posible impacto adverso en las personas, incluida la intrusión en su privacidad. Al examinar a la luz estos criterios el uso de drones por usuarios / ciudadanos privados que desarrollan actividades privadas o como un pasatiempo, y el tratamiento resultante de datos personales, se podría llegar a la conclusión de que el tratamiento llevado a cabo a través de los drones podría cumplir varios de estos criterios quedando entonces su uso fuera del alcance de la excepción de ámbito doméstico. Por ejemplo, hay que entender que los datos personales pueden divulgarse a un número indefinido de personas, en lugar de a una comunidad limitada de amigos, familiares o conocidos cuando se grabó con drones una película de una ciudad francesa que se publicó en un sitio web para compartir videos. Además, si los drones se utilizaran con fines privados en áreas públicas, es probable que muchas personas sin relación personal con el piloto se sientan afectados al ver que sus datos son recogidos. La escala y la frecuencia pueden variar mucho dependiendo de si los aficionados se unen a clubes y asociaciones actuando, a veces, pero no necesariamente y sistemáticamente, de manera colectiva y organizada.

Igualmente hay que referirse a la excepción relativa a la libertad de expresión por los medios periodísticos[38]. El tratamiento de datos personales realizado por medio de drones por razones periodísticas debe tener en cuenta las diferentes leyes y disposiciones nacionales que se aplican a este tipo de tratamiento. Sin embargo, los Estados miembros deben ser conscientes de la potencial capacidad de intromisión que poseen estos instrumentos, especialmente si se utilizan de forma irresponsable y poco ética, y deben identificar claramente los deberes y responsabilidades que conlleva el ejercicio de la libertad de expresión con la ayuda de drones. Como aclara el TJUE en el asunto Satamedia antes citado, "las actividades [...] pueden ser clasificadas como "actividades periodísticas" si su objeto es la divulgación al público de información, opiniones o ideas, independientemente del medio que se utilice para transmitirlos"[39]. En el LIBE y en el Informe del SEPD se ha recordado que la publicación de meros datos o imágenes obtenidas en Internet o en medios de comunicación, sin ningún fin informativo específico, no entrará dentro de la excepción de periodismo establecida en el *Artículo 9. "Tratamiento de datos y libertad de expresión"*[40] de la ya derogada Directiva 46/95. Lo cierto es que, para evitar problemas transfronterizos que pueden surgir debido a discrepancias, el SEPD aconsejó que la Comisión colaborara estrechamente con el Grupo de Trabajo del artículo 29 en la orientación específicamente relacionada con el uso de drones por los periodistas.

El Grupo de Trabajo del artículo 29 concede la máxima importancia a la introducción de un marco apropiado en el nivel nacional (si no está ya en funcionamiento) para que el uso de drones con fines estrictamente personales y recreativos y con fines periodísticos[41] no afecte a los derechos fundamentales a la privacidad o confidencialidad de las

comunicaciones y que se pueda garantizar el respeto de una expectativa razonable de protección de la vida privada, incluso en el caso de la recogida de datos personales llevados a cabo en lugares públicos. Como lo recordó el Tribunal Europeo de Derechos Humanos, existe una "zona de interacción de una persona con otras, incluso en un contexto público, que puede estar dentro del ámbito de la vida privada"[42].

3.3 Uso legítimo y proporcionado

En la Comunicación de 2014 y en el LIBE se ha recordado la necesidad de que el tratamiento de datos personales con el uso de drones solo se considerará justificado cuando persigan un fin legítimo, explícito o por motivos justificados, necesario en un estado democrático y la medida de tomada pueda considerarse proporcionada al propósito perseguido[43].

El tratamiento de datos personales relacionado con la aplicación civil de la tecnología de drones debe ser lícito con base en el artículo 6.1 del Reglamento, el cual dispone que éste será el caso si se cumple al menos una de las siguientes condiciones:

1º) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos. El consentimiento podría ser una base legal apropiada 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 espectadores presentes) [44].

2º) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación solicitada de este de medidas precontractuales. Por ejemplo, cuando alguien compra un producto que el vendedor entrega en su domicilio a través de un dron, o cuando los servicios de grabación de vídeo solo están relacionados con las propiedades de los interesados y son propuestos por compañías que operan drones. Sin embargo, se debe considerar que el tratamiento incidental de datos de terceros no afectados nunca está cubierto por el cumplimiento de obligaciones para las partes de un contrato y, por lo tanto, en los ejemplos anteriores, debe evitarse la recopilación de datos personales de terceros o se debe encontrar una base legal diferente para legitimarlo.

3º) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento.

4º) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

Estas dos últimas bases jurídicas podrían basarse en casos en los que el controlador deba cumplir una obligación legal impuesta por la ley, como la vigilancia de un sitio

arqueológico requerido por una disposición específica o, por ejemplo, en algunos "usos relacionados con la seguridad" (como el control del contrabando).

5º) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño. (es previsible que dichos criterios podría contemplarse, por ejemplo, en el caso de una operación de drones necesaria para la inspección de tuberías o líneas eléctricas o para la vigilancia de una infraestructura crítica o fotogrametría aérea, investigación atmosférica y meteorológica, control de energía eólica, seguimiento de huracanes, elaboración de mapas de sitios arqueológicos, control de hielo marino, investigación de vida silvestre, etc)[45].

Estas tres últimas bases jurídicas podrían interpretarse de manera flexible atendiendo a las circunstancias del caso.

6º) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física. Esta base legal podría ser relevante en algunos casos de "usos relacionados con la seguridad" como prestar socorro en caso de desastre o rescate (víctimas de accidentes de montaña o atrapados por la nieve), la inspección de un incendio, etc. Debe siempre interpretarse de forma estricta.

Pero que haya un fin legítimo no basta. Igualmente es necesario que se respete el principio de proporcionalidad. Es decir, es necesario que todas las intromisiones sean necesarias y proporcionadas en relación con el objetivo que se pretende alcanzar. Esto implica varias cosas. Los datos personales solo se procesarán si, y mientras, los fines no pueden cumplirse tratando información que no involucre datos personales. Se aplica aquí, el principio de minimización de datos. Hay que recordar que las limitaciones a los derechos fundamentales deben interpretarse de manera restrictiva, siguiendo la jurisprudencia del TEDH y del TJUE.

Habrá que elegir la tecnología más proporcionada y menos intrusiva[46], por ejemplo, aplicando técnicas de “anonimización”, tal como se establece en la Opinión 05/2014 sobre Técnicas de Anonimización[47]. En este sentido es importante la aplicación de la protección de datos mediante medidas predeterminadas que hagan más efectivo el amparo de la privacidad, en lugar de tener que actuar a posteriori[48]. Esto implica que, de antemano, los fabricantes y operadores respeten el denominado principio de protección de datos desde el diseño, tal como estipula el artículo 25 del Reglamento 2016/679[49]. La Comisión debería incentivarles a tener en cuenta esto siempre que el producto que se está diseñando tenga un uso conocido potencialmente grave para la intimidad como los sistemas completos de control o vigilancia. Es decir, en el nivel práctico, los fabricantes deben

integrar la protección de datos en todo el ciclo de vida de la tecnología, desde la etapa de diseño inicial, hasta su ejecución y uso. Esto significa analizar en las primeras etapas de desarrollo cómo su dispositivo podría interferir con la privacidad de los individuos, de modo que luego puedan construirlos de una manera que reduzca dicha interferencia a lo estrictamente necesario y proporcionado al propósito perseguido. De este modo, la tecnología del dron debe diseñarse de forma que evite el tratamiento de datos personales innecesarios. Finalmente, también se ha propuesto involucrar a un Oficial de Protección de Datos (cuando esté disponible) en el diseño e implementación de políticas relacionadas con el uso de drones.

Igualmente se deben adoptar medidas de protección de datos y privacidad por defecto, tal como estipula el artículo 25 del Reglamento 2016/679, es decir, configurando servicios y productos que deberían evitar la recogida o el tratamiento de datos personales innecesarios[50].

Además, si los datos se almacenan a bordo de un dispositivo deben guardarse de la forma más segura posible. Si no, deben eliminarse tan pronto como sea razonablemente posible. Y es que el almacenamiento a largo plazo de los datos recopilados en un dispositivo implica correr riesgos innecesarios por la posibilidad de que ocurra su pérdida o robo en una misión de vuelo posterior. Por último, hay que eliminar o anonimizar cualquier dato personal innecesario poco después de su recogida o tan pronto como sea posible.

Del mismo modo se ha subrayado la importancia de introducir, como parte del marco anterior, normas específicas que garanticen un uso responsable de los drones, lo que necesariamente debe incluir el respeto por las áreas privadas (como jardines, patios, terrazas, etc.) y por una "expectativa razonable" de privacidad, incluso algunas áreas públicas. Es decir, al planificar y operar un vuelo, incluso cuando se permita operar el dron sobre áreas pobladas, se tiene que evitar en la medida de lo posible volar sobre o cerca de áreas y edificios privados. Con dicho fin se ha propuesto prever, cuando sea necesario, la existencia de perímetros virtuales, o zonas de exclusión aérea. Además, dado que el uso de drones puede limitarse a áreas muy específicas en muchos Estados miembros, la publicación de mapas por las autoridades competentes ayudaría a los usuarios a comprender dónde está permitido el uso de drones[51].

Dado que los datos personales solo pueden tratarse si son adecuados, relevantes y no excesivos en relación con los fines para los que se recogen, debe realizarse una evaluación estricta de la necesidad y la proporcionalidad de los datos procesados[52]. Dada la variedad de aplicaciones de drones, desde el Grupo de Trabajo del artículo 29 se ha animado a los responsables políticos competentes, tanto en el nivel europeo como en el nacional, en estrecha consulta con los representantes de la industria, a que, al abordar el nuevo marco legal para la integración de los drones en el espacio aéreo civil europeo, fomenten, como una buena práctica, la realización de evaluaciones de impacto sobre los derechos y la libertad de las personas y, en particular, sobre el derecho a la privacidad y la protección de datos que la industria y los operadores pueden utilizar fácilmente. También el SEPD

insistiría en que los usuarios de drones (ciudadanos, empresas, administraciones, profesionales, agentes del orden público, servicios de inteligencia ...) deberían conocer el impacto de sus acciones en la privacidad, analizar sus necesidades e implementar procesos relacionados con el uso de drones de tal manera que la privacidad se vea menos afectada[53]. En particular, dado que las normas de protección de datos deben respetarse en la medida en que se procesen datos personales, se debe prever una evaluación de impacto de privacidad y protección de datos para los fabricantes en casos de drones "diseñados y producidos" con fines de vigilancia y para operadores que utilizan drones que llevan a bordo cualquier tipo de equipo "audiovisual". Siempre teniendo en cuenta, como se dijo antes, las cargas útiles y los fines de la recogida y el posterior tratamiento de datos personales, para cada tipo de operación de drones que puede involucrar dicho tratamiento de datos personales. Y todo ello a la luz de los riesgos previsibles derivados de los usos previstos, al proporcionar también a los interesados (fabricantes y operadores) un conjunto de criterios fáciles de usar para descubrir los riesgos de privacidad (si los hay) asociados con el uso de nuevas aplicaciones y evaluar si el tratamiento de datos personales a través de drones es legítimo, necesario y proporcionado al objetivo. De esta manera se trata de cubrir, entre otros, problemas y aspectos de transparencia y seguridad y documentación de los pasos tomados para abordar esos riesgos. Se recomienda evaluar el impacto de la protección de datos teniendo en cuenta el propósito de las operaciones y el tipo de drones involucrado en ellas (dimensión, visibilidad, etc.) y las combinaciones específicas de tecnología de detección a bordo. Hay que identificar la base legal más adecuada (consentimiento de los interesados, cumplimiento de un contrato, obligación legal, interés legítimo, etc.) de acuerdo con la ley nacional de protección de datos y la posible necesidad de notificar / consultar a las autoridades de protección de datos competentes, identificar fácilmente a la persona que opera el dron[54] e informar debidamente a las personas sobre el tratamiento de sus datos personales y sobre las modalidades para ejercer sus derechos. El análisis de posibles problemas de privacidad es clave para el desarrollo y uso de los drones y debe guiar los procesos comerciales y las elecciones tecnológicas[55].

3.4 *El problema de la información al ciudadano y la conservación de los datos*

De conformidad con el principio del tratamiento justo (arts.12 y ss del Reglamento 2016/679), los interesados deben conocer cuando se recogen y tratan sus datos personales. De acuerdo con el art.13 del citado Reglamento cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación[56]:

> *la identidad del controlador del dron y de su representante, los fines del tratamiento para el cual están destinados los datos y su base jurídica, cualquier información adicional, como las destinatarios o categorías de destinatarios de los datos, el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los*

criterios utilizados para determinar este plazo, la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado a los registros visuales y no visuales que los conciernen, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos, el derecho a presentar una reclamación ante una autoridad de control, etc[57].

Dicha información podría localizarse dentro de la propia página web de los proveedores. El Grupo de Trabajo de artículo 29 reconoce que el uso de drones plantea un desafío sobre cómo proporcionar información sobre su presencia o cómo hacer que los posibles afectados o interesados puedan consultar esa información de forma anticipada. El problema principal es que, a veces, su presencia es tan invisible que no se notará y mucho menos se podrá saber que está recogiendo datos. Para cumplir con este requisito de transparencia e información para los sujetos afectados se debe considerar un enfoque multicanal (es decir, tratar de garantizar que la información se transmite a través de varios medios de comunicación). Así, se han propuesto varias posibilidades.

En primer lugar, para operaciones de drones en lugares fijos[58] (como eventos deportivos, conciertos, áreas arqueológicas, parques naturales, etc.) los medios habituales parecen útiles. Con carácter previo, la organización del evento, el gestor del lugar o la persona interesada podrían informar al público por medio de las redes sociales, sitios web, periódicos, folletos o carteles, programas en medios audiovisuales[59] o envíos por correo en un buzón[60]. En el mismo lugar se puede acudir fácilmente a los tradicionales carteles u hojas de información, así como a los elementos de exhibición pública (por ejemplo, pantallas de televisión en un estadio deportivo), emisión de señales inalámbrica emitida, luces intermitentes, timbres y colores brillantes. Estos mismos medios pueden ser útiles en el caso de que el dron sobrevuele un espacio público sin claras limitaciones del alcance territorial donde la información a los sujetos cuyos datos potencialmente se pueden tomar resulta difícil o absolutamente imposible, (por ejemplo, cuando los drones se utilizan para vigilar grandes infraestructuras como redes ferroviarias o redes eléctricas)[61]. En este supuesto también se ha planteado la creación de un recurso que proporcione información en el nivel nacional o transnacional (más fácil de encontrar que los sitios web de operadores individuales) [62] para permitir que las personas interesadas puedan identificar las misiones concretas y los operadores de drones individuales que les afecten[63]. Todo ello con el fin de hacer visible e identificable el dron y su operador en la medida de lo posible[64].

En segundo lugar, se podría exigir el requisito de que el dron lleve una marca de registro (similar a la matrícula del vehículo). Esta medida solo es relevante en la medida en que los drones sean visibles desde el suelo o si hay una pérdida de control y se puede acceder a un aparato accidentado, por ejemplo. Se ha reconocido la conveniencia de una solución de este tipo pues, de este modo, los datos almacenados pueden vincularse con un operador concreto. Igualmente se comenta exigir la transmisión de una señal de marca de registro

inalámbrico que se puede conectar con una base de datos en línea. No obstante, también deben tenerse en cuenta las preocupaciones que genera con relación a la protección y seguridad de los datos un sistema de registro.

En tercer lugar, se recomienda que los operadores de drones publiquen información en su sitio web o en plataformas especializadas en informar regularmente sobre las diferentes operaciones que han llevado a cabo o piensan realizar[65].

En cuarto lugar, como hacen algunos Estados miembros, sería interesante la publicación por las autoridades de una lista de operadores autorizados para hacer un uso profesional de los drones y / o que cuentan con una autorización otorgada para cada operación. Se ven muy positivamente este tipo de listas ya que pueden facilitar el acceso a la información sobre operaciones que pueden implicar un tratamiento de datos.

En quinto lugar, teniendo en cuenta que en muchos Estados miembros no está permitido por diferentes motivos operar drones en algunas áreas, la publicación de mapas[66] que muestran las áreas donde los drones pueden ser utilizados sería muy útil. Y es que la publicación de este mapa ayudaría a las personas afectadas potencialmente a identificar las áreas en las que los drones podrían estar operando.

Finalmente, el Grupo de Trabajo del artículo 29 recomienda que la Comisión Europea haga uso de sus programas de financiación para apoyar investigaciones e inversiones de nuevas tecnologías destinadas a aumentar la transparencia. Se trata de potenciar nuevas tecnologías que faciliten informar al público en general sobre los drones y sobre cómo ejercer sus derechos de acceso. De este modo se promoverían, por ejemplo, placas o matriculas inteligentes o sitios web que publicarían información en tiempo real sobre todas las operaciones con drones.

En cuanto al tema de la conservación de los datos los controladores y los encargados del tratamiento de los datos, en su caso, deben aplicar las medidas técnicas y organizativas adecuadas para proteger dicho tratamiento contra la destrucción accidental o ilegal o pérdida accidental o alteración no autorizada[67]. Esta disposición también se aplica a los ataques electrónicos y cibernéticos (es decir, la manipulación remota del dispositivo para tomar el control total o parcialmente sobre él o para obtener acceso a los sensores o a los datos almacenados). Esta protección igualmente debe proporcionarse en la fase de transmisión de los datos personales desde el dron a la estación base. Se recomienda que los diseñadores de drones y equipos adaptados para ser ensamblados al dron interactúen con expertos de seguridad especializados en garantizar que las vulnerabilidades de seguridad se aborden adecuadamente. Además, se subraya que los datos personales tratados a través de drones no deberían almacenarse durante un período más prolongado de lo estrictamente necesario para su tratamiento[68]. Por consiguiente, aquellos datos que no estén vinculados a una queja o problema deberían eliminarse o anonimizarse

inmediatamente después de haber sido tomados. A este respecto se apunta que la incorporación de programas de almacenamiento y eliminación podría ser aconsejable. Por lo tanto, los dispositivos que transportan los drones deben diseñarse de manera que permitan establecer un período de almacenamiento definido de los datos personales recopilados y, como resultado, la eliminación automática regular de dichos datos personales que ya no es necesaria[69].

3.5 La garantía de la formación del operador del dron

Las personas que operan los drones no sólo deben saber pilotarlos sino también conocer las posibles consecuencias de su uso sobre los derechos de las personas a la privacidad y la protección de datos. Desde luego, se recomienda la introducción de aspectos de protección de datos entre las características clave de las disposiciones nacionales que regulan el uso comercial de drones (en relación con la capacitación de pilotos, los requisitos de aeronavegabilidad y certificación, la emisión / revocación de licencias de operación y permisos de trabajo aéreo, etc.) solicitando una cooperación estricta entre las Autoridades de Protección de Datos y las autoridades aeronáuticas. Parece ser que en algunos países[70], de una u otra manera, se ha impuesto la necesidad de probar que se conocen los requisitos para garantizar la protección de datos.

Quizás la medida más efectiva en este terreno sea exigir que todo aquél que desee contar con una autorización de vuelo de un dron demuestre que posee unos conocimientos mínimos y previos sobre la legislación de privacidad y protección de datos, para garantizar que los pilotos conozcan las obligaciones legales en el caso de que se produzca un tratamiento de datos personales. De este modo, en algunos casos esta materia ya forma parte de los exámenes que llevan a cabo las autoridades aeronáuticas competentes al otorgar permisos para operar aeronaves de este tipo.

Esa prueba de que se posee esa formación también podría alcanzarse informando a la autoridad competente de haber tenido en cuenta todos los requisitos establecidos por la legislación de protección de datos como parte de las condiciones bajo las cuales se otorgará un permiso[71]. Se trata de una buena práctica que debe apoyarse ya que podría ayudar a llamar la atención de los operadores sobre los aspectos relacionados con la protección de datos antes de cualquier vuelo autorizado y podría ayudar a realizar una base de datos central públicamente disponible en la que, al menos, figurase una lista de operadores (incluida una descripción genérica de los fines para los que podrían tratar los datos personales). Esto no significa que las autoridades asuman la responsabilidad de verificar que el operador del dron haya tomado todas las medidas adecuadas para cumplir con la legislación nacional de protección de datos (funcionando como una especia de declaración responsable parcial relativa a un requisito concreto de los varios obligatorios para obtener una autorización de vuelo). Pero es un punto de control útil que obligará al operador del dron a tomar una decisión consciente con respecto a su deber de actuar respetando el derecho a la protección de datos de los posibles afectados.

Igualmente se ha sugerido prever códigos de conducta y / o esquemas de certificación para fabricantes y operadores de la industria con el fin de mejorar la conciencia y comprensión o aceptabilidad social de los operadores de drones civiles sobre cuestiones de protección de datos y con el fin de ayudar a las autoridades a controlar su cumplimiento previniéndose la comisión de infracciones. El papel importante que los Códigos de conducta[72] pueden tener en este marco es aún más interesante teniendo en cuenta que las autoridades de protección de datos no pueden evaluar ni perseguir infracciones de privacidad más amplias cuando van más allá de sus facultades legales. Dichos Códigos deben contener sanciones en caso de que los signatarios no lo cumplan. En cuanto a la promoción de certificaciones de protección de datos, se trata de lograr el fin de mejorar la conciencia y la comprensión de los operadores de drones civiles sobre los problemas de protección de datos, así como el objetivo de supervisar el cumplimiento normativo[73].

Finalmente, no hay que descartar otras medidas para llamar la atención del usuario sobre la necesidad de respetar la protección de datos y otras normas nacionales. Así hay que referirse a la implantación de cursos de capacitación, eventos públicos y, muy especialmente, a la distribución de un folleto junto con el dron que se comercializa[74]. En relación con esto último, se ha sugerido la introducción de una obligación, en el nivel europeo y / o nacional, para que los fabricantes que comercialicen o venden únicamente drones pequeños a usuarios finales privados o profesionales lo hagan empaquetados conjuntamente con información suficiente o "avisos de privacidad" (por ejemplo, dentro de las instrucciones de funcionamiento) sobre la posible intrusión de estas tecnologías y recordando la necesidad de respetar la legislación y las reglamentaciones europeas y nacionales que protegen la privacidad, los datos personales y otros derechos fundamentales.

Para terminar con este apartado hay que señalar que para el LIBE era muy importante recomendar a las instituciones la creación de un marco normativo más concreto en torno al uso civil de drones. Solo de esta forma se podría transmitir a los usuarios información suficiente para que estos conocieran el potencial intrusismo de estas tecnologías en los derechos fundamentales de vida privada y protección de datos de los ciudadanos.

4. USO DE DRONES CON FINES DE SEGURIDAD PÚBLICA

Ha aclarado el Grupo de Trabajo del artículo 29 que los rápidos avances tecnológicos y la alta capacidad de controlar objetivos y transmitir datos en tiempo real, han llamado la atención de los gobiernos nacionales y supranacionales que buscan un uso de los drones más encaminada a la vigilancia, seguridad y prevención del terrorismo, que a un uso militar[75]. Su aplicación en las medidas de seguridad nacional ha sido valorada positivamente por los organismos de control del respeto a los derechos fundamentales,

siempre que se destine al control de "áreas donde la expectativa individual de privacidad no esté bien definida". También se señala que los aviones no tripulados pueden indicar una transformación fundamental de las prácticas policiales, en particular con respecto al papel de los datos en la orientación de las acciones de aplicación de la ley, que van desde controlar a un individuo hasta determinar los objetivos a partir de una revisión de las vidas y actividades de una población específica basado en la vigilancia continua.

Ahora bien, si esta tecnología es muy atractiva para la persecución del crimen y las infracciones administrativas, en la misma medida constituye un potencial problema para los derechos de los ciudadanos. La Unión Americana de Libertades Civiles se opone a la realización rutinaria de sesiones de vigilancia aérea sobre población civil, pues entiende que otorga un poder demasiado extenso al Estado, el cual estaría capacitado para controlar, seguir y grabar a cualquier individuo en su día a día, convirtiéndose en un espía de sus propios ciudadanos[76]. Además, hay que preguntarse qué uso se hace de los datos personales registrados por medio de drones por la policía y otras autoridades encargadas de hacer cumplir la ley.

Es verdad que de conformidad con el artículo 4, apartado 2, del Tratado de la Unión Europea "la seguridad nacional es responsabilidad exclusiva de cada Estado miembro y debe ser respetada por las instituciones comunitarias. Pero que la seguridad pública sea de su competencia, esto no significa que deban olvidarse de otras exigencias superiores que vienen del mismo Derecho comunitario y europeo. Por eso el Grupo de Trabajo del artículo 29 advierte que el uso de drones operados directamente por la policía y otras autoridades encargadas del orden público -o su solicitud de acceso a datos recolectados por drones operados por entidades privadas para sus propios fines- crea altos riesgos para los derechos y libertades de las personas e interfiere directamente con el los derechos al respeto de la vida privada y a la protección de los datos personales protegidos por el artículo 8 del Convenio Europeo de Derechos Humanos y la jurisprudencia correspondiente del TEDH los artículos 7, 8 y 52.1 de la Carta Europea de los Derechos Fundamentales El tratamiento de datos personales por parte de las fuerzas del orden también se rige por los artículos 7 y 8 de la Carta y el artículo 16 del TFUE. Por su parte el LIBE recuerda, a la luz de la jurisprudencia del TJUE, la necesidad de interpretar de manera estricta el citado artículo 4.2[77] y que, asimismo, en el marco de la vigilancia por parte de las autoridades nacionales, se recomendaba a éstas el cumplimiento de las normas de protección de los derechos fundamentales. El TJUE ha confirmado que el uso de drones para fines no incluidos en el alcance del Tratado, como la seguridad nacional, deben cumplir, con estas reglas europeas[78].

Por eso el Grupo de Trabajo del artículo 29 ha recordado que se deben cumplir los mismos requisitos, de forma similar al uso de drones con fines comerciales, que en el caso de que el manejo del dron se realice por personas privadas.

Por tanto, para empezar, esta limitación al ejercicio de los derechos y libertades procedente de la policía al utilizar los drones debe estar prevista por la ley ("de conformidad con la ley"), cumpliendo genuinamente los objetivos de interés general reconocidos por la Unión o la necesidad de proteger los derechos y las libertades de los demás ("en cumplimiento de uno de los objetivos legítimos establecidos en el artículo 8 (2) del Convenio citado y de los necesarios en una sociedad democrática" que responda a una "urgente necesidad social"[79]). Por tanto, la policía y otras autoridades policiales que usan drones deben asegurarse de tener una base legal válida para tratar los datos personales. Esto implica respetar el principio de transparencia. Es decir, el tratamiento de datos realizado mediante el uso de drones debe establecerse o prescribirse por ley para que sea transparente y previsible para los interesados. La ley debe ser accesible para que, dada su publicidad, todos ciudadanos puedan obtener información sobre cómo pueden interferir en sus derechos la actuación policial. Esta ley también debe ser previsible, es decir, suficientemente clara y detallada para que el ciudadano pueda prever cuándo es probable que estén sujetos a medidas. Por supuesto este sometimiento al Derecho cubre lo dispuesto en instrumentos internacionales específicos en los que todos los Estados miembros de la UE son parte. En particular, en la medida en que se procesan datos personales, cabe recordar aquí de nuevo los requisitos establecidos en el Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos personales, que también proporciona salvaguardias relevantes, y en la Recomendación n° R (87) 15 del Comité de Ministros a los Estados miembros, adoptada por el Comité de Ministros el 17 de septiembre de 1987, que regulan el uso de datos personales en el sector policial deben ser cumplidas por las autoridades que procesan los datos personales para la aplicación de la ley por motivos de seguridad nacional[80]. Finalmente, hay que recordar una vez más el papel que juegan los tribunales que controlarán que el uso de drones con fines de inteligencia se ajuste a la legalidad[81]. Como resultado de todo esto, cualquier tratamiento intrusivo por parte de las autoridades encargadas de hacer cumplir la ley debe estar sujeto a las salvaguardias de protección de datos evocadas por el TJUE en la sentencia Derechos Digitales Irlanda c. Seitlinger arriba citada.

Una vez cubierto el requisito formal del principio de reserva de ley, la siguiente exigencia inevitable es el respeto escrupuloso a los principios de necesidad, proporcionalidad, idoneidad en la toma de medidas vulneradoras de estos derechos. Como dice el SEPD en su Informe citado, en particular, debería garantizarse que las autoridades encargadas de hacer cumplir la ley solo utilicen un dron en el marco de una investigación específica cuando su uso se considere necesario y cuando ningún otro medio menos intrusivo logre el mismo propósito[82]. Los aviones no tripulados solo se utilizarán cuando se ofrezca una demostración concreta de su necesidad e idoneidad para los fines específicos perseguidos estrictamente enumerados por adelantado, justificados y establecidos en la legislación pertinente[83]. Es decir, las autoridades han de justificar por qué los instrumentos existentes a su disposición y por qué las alternativas menos intrusivas no lograrán dicho objetivo

(una evaluación previa por parte de las Autoridades de Protección de Datos puede ser aplicable y podría preverse para este propósito cuando las prácticas nacionales favorezcan dicha evaluación previa). Según el Grupo de Trabajo del artículo 29, en cualquier caso, el uso debe estar geográficamente confinado y limitado en el tiempo. No se debe permitir el rastreo constante, indiscriminado o masivo de personas. Si el seguimiento constante es estrictamente necesario debe restringirse a investigaciones garantizadas por la ley. Hay que imponer límites al uso de drones para actividades de vigilancia con el objetivo de evitar que se agrupen datos y se elaboren perfiles que se utilicen para señalar objetivos basados en el análisis de datos. Con vistas al efecto que puede tener el uso de drones sobre los derechos a la libertad de expresión y la libertad de reunión, se debe prestar especial atención a la necesidad de proteger, en la medida de lo posible, las manifestaciones públicas y reuniones similares de cualquier tipo de vigilancia. El equipo técnico y de detección utilizado debe estar en consonancia con el objetivo del tratamiento. La prohibición de la aplicación automática de decisiones también se aplica a estos usos. Los datos procesados a través de drones deberían ser analizados por un operador humano antes de tomar cualquier decisión que afecte negativamente a un individuo.

Cuando las autoridades encargadas de hacer cumplir la ley traten los datos recopilados por los drones para la ejecución de delitos civiles, deberán cumplir los requisitos establecidos por el Reglamento. En la medida de lo posible, los interesados deben ser informados del tratamiento y sus derechos correspondientes. Los métodos y tipos de usos de los drones por parte de las autoridades encargadas de hacer cumplir la ley no deberían ser secretos. Dependiendo de la legislación nacional, los datos personales recopilados mediante el uso de drones para este tipo de investigaciones deben incorporarse en los archivos administrativos que se pueden utilizar en los tribunales.

BIBLIOGRAFÍA

ALONSO GARCÍA, R: "La carta de los derechos fundamentales de la Unión Europea", *Gaceta jurídica de la Unión Europea y de la competencia,* Nº 209, 2000, pp. 3-17.

BLASI CASAGRAN, C: "El empleo emergente de drones con fines policiales en la Unión Europea: avances y limitaciones", Julio, 10, 2014, http://www.seguridadinternacional.es/?q=es/content/el-empleo-emergente-de-drones-con-fines-policiales-en-la-unión-europea-avances-y-limitaciones.

CLARKE, R: "Regulación del impacto de los aviones no tripulados civiles en la privacidad del comportamiento", *Computer Law & Security Review* 30, 3 de junio de 2014.

DOMÉNECH, G: *"Derecho de la información",* Ed. Publixed, 2014.

ELORDI VILLENA, M: "El uso de vehículos aéreos no tripulados (drones) en las labores de seguridad y vigilancia de la Administración (Protección de la intimidad y responsabilidad de las Administraciones Públicas", en Congreso Derecho TICs-SICARM 2014: Innovación, tecnología y gestión avanzada de la información administrativa. Implicaciones jurídicas del cambio de paradigma.

ESCRIBANO TORTAJADA, P: "Drones y derecho a la intimidad y la propia imagen: estado de la cuestión y problemas que se plantean en la actualidad", pp.238-259, en *"El derecho aéreo entre lo público y lo privado (Aeropuertos, acceso al mercado, drones y responsabilidad)",* Ed. Universidad Internacional de Andalucía, 2017.

FINN, R.L, WRIGHT, D, DONOVAN, D, JACQUES, L y DE HERT, P: "*Privacy, data protection and ethical risks in civil RPAS operations*". D3.3: Final report of the European Commission. Available at http://ec.europa.eu/DocsRoom/documents/8550 (Accessed April 10, 2016).

GÓMEZ-JUÁREZ SIDERA, I.DEL: "Drones y privacidad: desafíos de la protección de datos en la utilización civil de aeronaves pilotadas por control remoto", *Fodertics 4.0,* Comares, Granada, 2015.

KOLEV, Z. (2012). *RPAS for European Border Surveillance. Challenges of Introducing RPAS Technology in an Operational Context.* Presentation, FRONTEX, Research and Development Unit, Paris. https://ico.org.uk/for-the-public/drones/. http://ec.europa.eu/DocsRoom/documents?locale=en&tags=Privacy%20and%20data%20protection%20policy%20for%20the%20civil%20use%20of%20drones.

MORA RUIZ, M: "La ordenación jurídico-administrativa de los drones en el Derecho español: entre la libre competencia y la protección del interés general", pp.210-237, en *"El derecho aéreo entre lo público y lo privado (Aeropuertos, acceso al mercado, drones y responsabilidad)",* Ed. Universidad Internacional de Andalucía, 2017.

MUÑOZ, T: "Los drones y la protección de datos de carácter personal", *Área Cumplimiento Normativo DGE Data,* http://www.dge.es/home/quienes-somos/548-los-drones-y-la-proteccion-de-datos-de-caracter-personal.

RODRIGUEZ ÁLVAREZ, J.L: "Los retos actuales de la protección de datos", en la obra *"20 años de protección de datos en España",* 2015, pp.453-470.

SARMIENTO RAMÍREZ-ESCUDERO, D: *"El "soft law" administrativo: un estudio de los efectos jurídicos de las normas no vinculantes de la Administración",* Cizur Menor, Navarra, Thomson Civitas, 2008.

REFERENCIAS

[1] Sobre el tema en general véase KOLEV, Z. (2012). *RPAS for European Border Surveillance. Challenges of Introducing RPAS Technology in an Operational Context.* Presentation, FRONTEX, Research and Development Unit, Paris. https://ico.org.uk/for-the-public/drones/. http://ec.europa.eu/DocsRoom/documents?locale=en&tags=Privacy%20and%20data%20protection%20policy%20for%20the%20civil%20use%20of%20drones y MUÑOZ, T: "Los drones y la protección de datos de carácter personal", *Área Cumplimiento Normativo DGE Data,* http://www.dge.es/home/quienes-somos/548-los-drones-y-la-proteccion-de-datos-de-caracter-personal. Esta autora señala que "con esta diversidad de posibilidades las empresas tienen por delante un gran reto legal, ya que el espacio aéreo regulado exige unos estándares de control y seguridad muy exigentes y ni Estados Unidos ni Europa permiten el vuelo de aviones totalmente autónomos y drones, en general. En el Consejo Europeo de diciembre de 2013, se habló de garantizar la integración progresiva del sistema de aeronaves teledirigidas en el espacio aéreo a partir de 2016. Cada país tiene su propio conjunto de problemas y restricciones legales a tener en cuenta antes del uso de drones. El uso de los drones está siendo visto con una creciente preocupación por parte de la sociedad civil lo cual hace necesaria una regulación específica que limite y proteja los derechos de la esfera privada de las personas". Ver también la investigación realizada entre las autoridades publicada por FINN, R.L, WRIGHT, D y DONOVAN, D (Trilateral Research & Consulting, LLP) y JACQUES, L y DE HERT, P (Vrije Universiteit Brussel), "*Privacy, data protection and ethical risks in civil RPAS operations*", p.145 y ss (en cuanto a una descripción de las legislaciones europeas y nacionales, p.363 y ss), en D3.3: Final report of the European Commission. Available at http://ec.europa.eu/DocsRoom/documents/8550 (Accessed April 10, 2016). En el ámbito de la doctrina española resulta de gran interés los excelentes estudios de MORA RUIZ, M: "La ordenación jurídico-administrativa de los drones en el Derecho español: entre la libre competencia y la protección del interés general", p.210 y ss y ESCRIBANO TORTAJADA, P: "Drones y derecho a la intimidad y la propia imagen: estado de la cuestión y problemas que se plantean en la actualidad", p.238 y ss, ambos publicados en el volumen colectivo: *"El derecho aéreo entre lo público y lo privado (Aeropuertos, acceso al mercado, drones y responsabilidad)",* Ed. Universidad Internacional de Andalucía, 2017.

[2] Recientemente en la prensa se explica que la «startup» china Ehang ha publicado por primera vez un vídeo de uno sus drones volando con personas a bordo. Se trata de un taxi aéreo autónomo: el Ehang 184. Los pasajeros no pilotan el dron, que es controlado desde una base, aunque inicialmente, por su cuenta, identifica un lugar desde donde despegar y aterrizar

[3] Ver Reglamento (CE) Nº 216/2008 del Parlamento Europeo y del Consejo, de 20 de febrero de 2008 sobre normas comunes en el ámbito de la aviación civil y por el que se crea una Agencia Europea de Seguridad Aérea, y se deroga la Directiva 91/670/CEE del Consejo, el Reglamento (CE) Nº 1592/2002 y la Directiva 2004/36/CE

[4] Ver *'Prototype' Commission Regulation on Unmanned Aircraft Operations"*, 22 de agosto 2016. https://www.easa.europa.eu/system/files/dfu/UAS%20Prototype%20Regulation%20final.pdf. En este proyecto legislativo se enumeraban algunos de los requisitos que deberán respetarse en manejo de drones: Los pilotos de alta gama deberán registrarse formalmente para obtener una licencia que les permita manejarlos. Los Estados Miembros podrán limitar e incluso prohibir el vuelo de estos aparatos en determinadas zonas, por razones de seguridad o especial peligrosidad. Los drones no deberán volar cerca de donde operen los servicios de emergencia; hospitales, parques de bomberos, comisarías de policía. Deberán cumplirse los requisitos de seguridad mínimos establecidos y otras exigencias técnicas e incluso podrá exigirse al propietario la contrata de un seguro de responsabilidad civil.

[5] Ver Informe técnico sobre la «Introducción de un marco regulador para el funcionamiento de drones», de 18 de diciembre de 2015 (https://www.easa.europa.eu/system/files/dfu/Introduction%20of%20a%20regulatory%20framework%20for%20the%20operation%20of%20unmanned%20aircraft.pdf).

[6] Ver COM/2014/0207 final. Ver también el Dictamen del 15 de octubre de 2014 del Comité Económico y Social Europeo

sobre la citada Comunicación (http://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/remotely-piloted-aircraft-systems).

[7] Sobre el tema es de imprescindible consulta el trabajo de ALONSO GARCÍA, R: "La carta de los derechos fundamentales de la Unión Europea", *Gaceta jurídica de la Unión Europea y de la competencia,* Nº 209, 2000, pp. 3-17.

[8] Ver Riga Declaration on remotely piloted aircraft (drones). "Framing the future of aviation" Riga - 6 March 2015 (https://ec.europa.eu/transport/sites/transport/files/modes/air/news/doc/2015-03-06-drones/2015-03-06-riga-declaration-drones.pdf).

[9] El denominado «Grupo de trabajo sobre protección de datos del artículo 29» (artículo 29 WP) se creó en virtud de la ya derogada Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, sobre la protección de las personas en lo que respecta al tratamiento de datos personales y sobre la libre circulación de tales datos. Tiene estatus consultivo y actúa de manera independiente. Está compuesto por un representante de la (s) autoridad (es) de supervisión designadas por cada Estado miembro de la UE, un representante de la (s) autoridad (es) establecida (s) para las instituciones y órganos de la UE y un representante de la Comisión Europea. Sus tareas se describían en el art.30 de la Directiva 95/46/EC y en el art.15 de la Directiva 2002/58/EC.

[10] Hay que advertir que hay muchos tipos de drones. Sus dimensiones pueden variar desde unos pocos centímetros hasta varios metros. Sus capacidades de vuelo también pueden ser muy diferentes, desde muy leves hasta poder llegar a alcanzar altas velocidades y altitud, como aviones de alto rendimiento. El control de drones por pilotos remotos generalmente se basa en enlaces de datos múltiples y enlaces de comando proporcionados por equipos de radio o enlaces de datos establecidos a través de Internet mediante enlaces de acceso inalámbrico digital, con los pilotos remotos trabajando en el suelo (o a bordo de otro vehículo). En muchos casos operan dentro de la línea de visión. Para las operaciones más allá de la línea de visión se requiere estrictamente un sistema de navegación que dependa de sistemas de posicionamiento como GPS, y equipo de telemetría para la conciencia situacional del piloto durante el vuelo, a veces enriquecido con imágenes en vivo de cámaras a bordo.

[11] Se recuerda que los drones comercialmente disponibles no están necesariamente equipados con cámaras a bordo u otros sensores por defecto y que la elección del operador de drones puede ser una opción, según el tipo de uso. Un dron también puede ser diseñado y construido por el propio operador que compra componentes de una variedad de proveedores.

[12] Su "movilidad y discreción" les permite ser utilizados en muchas más circunstancias que los sistemas de vuelo tripulados.

[13] Por ejemplo, los drones permiten capturar imágenes que no estarían disponibles si la cámara fuese fija (propiedades privadas con vallas altas, terrazas de alto nivel, jardín). Los equipados con cámaras de video obviamente comparten muchos puntos comunes con los sistemas de CCTV. Permiten la grabación continua o la activación de la grabación en función, por ejemplo, de la detección de movimiento. Sin embargo, su movilidad y discreción ofrece más y también usos cada vez más diferentes. En otras palabras, dan alas a las cámaras más sofisticadas. Además, a diferencia de las cámaras que son visibles la mayor parte del tiempo, los drones no siempre son visibles desde el nivel del suelo. Tanto su movilidad como su discreción facilitan el seguimiento de las personas. La necesidad de enmascarar partes de las zonas filmadas para respetar la privacidad de los individuos plantea más desafíos debido a su movilidad constante y sus posibilidades de zoom.

[14] RFID o identificación por radiofrecuencia (del inglés Radio Frequency Identification) es un sistema de almacenamiento y recuperación de datos remoto que usa dispositivos denominados etiquetas, tarjetas o transpondedores RFID. El propósito fundamental de la tecnología RFID es transmitir la identidad de un objeto (similar a un número de serie único) mediante ondas de radio. Las tecnologías RFID se agrupan

dentro de las denominadas Auto ID (*automatic identification*, o identificación automática).Las etiquetas RFID (*RFID tag* en inglés) son unos dispositivos pequeños, similares a una pegatina, que pueden ser adheridas o incorporadas a un producto, un animal o una persona. Contienen antenas para permitirles recibir y responder a peticiones por radiofrecuencia desde un emisor-receptor RFID. Ver https://es.wikipedia.org/wiki/RFID.

[15] El SEPD emitió un dictamen (de fecha 26 de noviembre de 2014) sobre la Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre "Una nueva era para la aviación - Apertura del mercado de la aviación al uso civil de sistemas de control remoto sistemas de aeronaves de manera segura y sostenible. Ver, http://ec.europa.eu/justice/data-protection/article-29/index_en.htm. Este dictamen se puede consultar en https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-11-26_Opinion_RPAS_EN.pdf. Este dictamen identifica varias situaciones en las que los drones procesan datos personales y en los que los controladores están, por lo tanto, sujetos al marco de protección de datos aplicable vigente. Pretende analizar todos los requisitos de protección de datos que deben cumplirse para los drones operativos. Esto puede estar sujeto a la orientación de las autoridades nacionales de protección de datos, del Grupo de Trabajo del artículo 29 o incluso del SEPD en su función de supervisión si las instituciones y organismos de la UE utilizaran drones para procesar datos personales. En vista de la necesidad imperiosa de garantizar el respeto de los requisitos de privacidad, protección de datos y seguridad relacionados con esta nueva tecnología potencialmente muy intrusiva, el SEPD respaldó que la Comisión reconsiderase su falta de competencia para la regulación de los drones de menos de 150 kilos.

[16] Ver sentencia del Tribunal de Justicia de la Unión Europea (en lo sucesivo TJUE) de 8 de abril de 2014, As Ac C-293/12 y C-594/12.

[17] Ver sentencia del TJUE de 13 de mayo de 2014, As C-131/12. Google España SL and Google Inc. c. Agencia Española de Protección de Datos and Mario Costeja González.

[18] Por ejemplo: 1º) Equipo de grabación visual: cámaras inteligentes con distancia focal fija o variable, capaz de almacenar y transmitir imágenes en vivo, con capacidades de reconocimiento facial a bordo o en tierra, permitiendo a los drones identificar y rastrear individuos, objetos o situaciones específicas, (las tecnologías integradas también podrían incluir la posibilidad de rastrear dispositivos que llevan chips RFID), identificar patrones de movimiento, para leer las matrículas de los vehículos, al tiempo que garantiza una vista de 360°, habilitada para detectar la energía térmica emitida por un objetivo, lo que permite el vuelo y la grabación de imágenes en condiciones de poca visibilidad (debido a niebla, humo o escombros) o durante las horas nocturnas; 2º) Equipo de detección: sensores óptico-electrónicos, escáneres de infrarrojos, radares de apertura sintética para identificar objetos, vehículos y embarcaciones y obtener información sobre su posición y rumbo incluso detrás de paredes, techos, humo u otros obstáculos; 3º) Equipo de radiofrecuencia: como antenas que capturan la ubicación de puntos de acceso Wi-Fi o estaciones celulares, femtocélulas y catcher IMSI utilizados por las fuerzas del orden para controlar teléfonos celulares y redes o por el proveedor de servicios para transmitir comunicaciones entre redes y usuarios de terminales; sistemas que leen las direcciones IP de todos los dispositivos ubicados en un edificio sobre el cual volará el dron; 4º) Sensores específicos para la detección de rastros nucleares, rastros biológicos, material químico, dispositivos explosivos.

[19] Ver arts.4 a) y 5 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, 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. Sobre la interpretación de la noción de dato, véase: Article 29 Data Protection Working Party, Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance, WP89, p. 15 y Opinion 04/2007 on the concept of personal data, WP136. "A Study on the Societal Impact" Annex to the "Roadmap for the integration of civil Remotely-Piloted Aircraft Systems into the European Aviation System".

[20] Ver Documento EASA 2017-05 (B), pp.27 a 29.

[21] Esto se conoce como el "chilling and panopticon effect syndrome" que se desprende del uso a gran escala de los drones.

[22] El SEPD en su Dictamen de 2014 ha explicado que en la UE, a diferencia de otros casos (véase la jurisprudencia estadounidense desarrollada sobre vigilancia aérea según la cual la policía puede volar válidamente, por ejemplo, sobre un jardín para detectar los elementos constitutivos de un delito. No hay intromisión en la privacidad de la persona porque 'cualquier miembro del público que vuele en este espacio aéreo que haya mirado hacia abajo podría haber visto todo lo que observaron estos oficiales'. Tribunal Supremo de los EE. UU., 1986, California c. Ciraolo), la ubicación en un espacio público o privado no es un criterio relevante para determinar si el derecho a la privacidad y el derecho a la protección de datos se aplica o no. Como recordó el Tribunal Europeo de Derechos Humanos en su sentencia de la Gran Sala Von Hannover c. Alemania (Nº. 40660/08 y 60641/08), de 7 de febrero de 2012, "el concepto de vida privada se extiende a aspectos relacionados con la identidad personal, como el nombre, la fotografía o la integridad física y moral de una persona; El artículo 8 del Convenio tiene como objetivo principal garantizar el desarrollo, sin injerencia externa, de la personalidad de cada persona en sus relaciones con otros seres humanos. Por lo tanto, existe una zona de interacción de una persona con otras, incluso en un entorno público. contexto, que puede caer dentro del ámbito de la vida privada. La publicación de una fotografía puede interferir en la vida privada de una persona, incluso cuando esa persona sea una figura pública" (véase el apartado 95 de la sentencia antes citada). El Tribunal reiteró que, "en determinadas circunstancias, incluso cuando una persona es conocida por el público en general, puede confiar en una" expectativa legítima "de protección y respeto de su vida privada" (véase el apartado 97 de la sentencia antes citada). Como resultado de todo ello, las personas en un espacio público, tanto particulares como personajes públicos, todavía pueden afirmar, por ejemplo, su derecho al respeto de su vida privada y familiar, es decir, el derecho a no ser enfocado con un objetivo zoom o direccional o un micrófono seguimiento o la grabación de sus conversaciones o a la protección contra la exposición de la totalidad de sus movimientos al público. En última instancia se recuerda que el aspecto de la protección de la intimidad exigirá un seguimiento continuo por parte de las autoridades competentes, incluidas las autoridades nacionales de supervisión de la protección de los datos personales.

[23] Ya ESCRIBANO TORTAJADA, P, op.cit, pp.244 y 248, nos recuerda que, aparte de la protección de datos, existen otros derechos que pueden verse vulnerados, centrándose en la propia imagen, la intimidad y la propiedad privada. Resulta de gran interés consultar su trabajo al plantear cuestiones muy relevantes que pueden derivarse del uso de los drones. Además, nos recuerda que la mayor preocupación a los ataques contra estos derechos puede venir de los drones más pequeños, “es decir, los micro o los nano drones, puesto que son casi imperceptibles para el ojo humano” y que las imágenes que pueden captar, por ejemplo, en las casas o jardines de los ciudadanos pueden ser subidas a internet.

[24] Ver Documento EASA 2015-10 (A-NPA), pp.48 a 50, donde se destaca lo siguiente: "Entre otros, la opinión también aborda recomendaciones a los responsables políticos 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, al introducir también normas específicas que garanticen un uso responsable de los drones (que debe incluir necesariamente el respeto por las áreas privadas)”.

[25] Además, tanto el SEPD como el Grupo de Trabajo del artículo 29 se han asociado en una fase temprana a la reflexión realizada por la Comisión sobre los drones. El SEPD desea continuar esta estrecha cooperación con la Comisión en el marco del Grupo de Trabajo del artículo 29 para garantizar, de forma armonizada, que los drones se utilizan de conformidad con los requisitos de protección de datos aplicables.

[26] La CNIL (Commission nationale de l'informatique et des libertés) publicó en Francia un documento de investigación sobre drones a finales de 2013 sobre este tema. El Comisionado de Información del Reino Unido igualmente está llevando a cabo una consulta para actualizar su código de prácticas de CCTV que ahora incluye una sección dedicada a los drones. La autoridad belga de protección de datos ha publicado un repertorio de preguntas frecuentes sobre este mismo tema en abril de 2014.

[27] Sobre la protección de datos en general puede verse RODRIGUEZ ÁLVAREZ, J.L: “Los retos actuales de la protección de datos”, en la obra *“20 años de protección de datos en España”,* 2015, pp.453-470. ESCRIBANO TORTAJADA, P, op.cit, p.244, advierte que “los drones pueden ser usados para tomar los datos personales de los ciudadanos y ser enviados a empresas para distintos fines”. Ver también GÓMEZ-JUÁREZ SIDERA, I.DEL: “Drones y privacidad: desafíos de la protección de datos en la utilización civil

de aeronaves pilotadas por control remoto", *Fodertics 4.0,* Comares, Granada, 2015.

[28] En la Declaración de Riga se deseaba que las autoridades responsables de protección de datos, tanto nacionales como europeas, desarrollasen directrices y mecanismos de supervisión necesarios para garantizar el pleno respeto de las normas de protección existentes en relación con los drones. Las reglas debían aclarar qué era aceptable y qué no, y requerían una aplicación adecuada. En el Informe del SEPD se dice que cuando los datos personales son tratados por drones operados en la UE, el marco legal de la UE para la protección de datos se aplica en principio. Su valor agregado para actividades como la agricultura, el periodismo o el control de infraestructuras es obvio, pero es crucial garantizar que, siempre que impliquen el tratamiento de datos personales, su uso cumpla con la ley de protección de datos.

[29] Incluidas las reglamentaciones nacionales sobre CCTV. A pesar de los diferentes impactos que el uso de drones puede tener sobre la privacidad y la libertad de las personas, en comparación con los sistemas de CCTV, puede haber circunstancias donde las disposiciones legales nacionales aplicables a los sistemas de CCTV también pueden aplicarse al uso de los drones, en particular en el caso de drones utilizados con fines de videovigilancia. A la luz de esto, el Grupo de Trabajo del artículo 29 se remite a su Opinión 4/2004 sobre el tratamiento de los datos personales mediante videovigilancia, haciendo hincapié en la actualidad del análisis jurídico y las recomendaciones que figuran en él. DOMÉNECH, G, en su excelente trabajo *"Derecho de la información",* Ed. Publixed, 2014. Tras analizar el tema de la protección de datos en general, explica la autora (p.158) que *"en la sociedad actual, los ciudadanos somos en la actualidad objeto de grabación continua por medio de circuitos cerrados de televisión, dispositivos webcam y de digitalización de imágenes, tanto en espacios públicos como privados. Pero esa seguridad que se pretende transmitir deriva en vigilancia encubierta y en captación continua de imágenes, incluso mediante cámaras instaladas en el lugar de trabajo, actividades en su conjunto que no pueden ser compatibles con los derechos reconocidos en la Constitución, lo que justifica su regulación".*

[30] Paralelamente, el tratamiento de los datos personales desencadena la aplicación del marco europeo de protección de datos, dondequiera que se lleve a cabo, ya sea en un espacio público o privado, siempre que el tratamiento tenga lugar en el contexto de las actividades de un establecimiento del controlador en la UE o con equipos o medios ubicados en la UE (Véase sentencia del TJUE de 6 de noviembre de 2003, Bodil Lindqvist, As C-101/01, apartados 46-47 y Declaración del Grupo de Trabajo del artículo 29 sobre los debates en curso sobre el paquete de reformas de protección de datos, 27.02.2013, disponible en http://ec.europa.eu/justice/data-protection/article29/documentation/other-document/files/2013/ 20130227_statement_dp_reform_package_en.pdf 9). Aunque los avances tecnológicos permitirían un aumento significativo de la vigilancia de las personas en el espacio público o incluso en espacios privados (como su casa, balcones o jardín) y el tratamiento de una mayor cantidad de datos personales, estos derechos se mantendrán y las salvaguardas que representan no se reducirán.

[31] Ver L 119/1, de 4.5.2016. Cualquier tratamiento de datos personales para un fin diferente del que se ha recopilado debe realizarse de conformidad con las disposiciones de la normativa y, por lo tanto, debe tener una base jurídica autónoma y su compatibilidad con el objetivo original también debe ser evaluado caso por caso. Ver Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation*, WP203. Sobre otro ejemplo significativo del uso incompatible de datos personales véase Article 29 Data Protection Working Party, *Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)*, Wp128, p. 15. Ver igualmente la Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre "El funcionamiento del puerto seguro desde la perspectiva de los ciudadanos y las empresas de la UE establecidos en la UE", https://secure.edps.europa.eu/EDPSWEB/webdav/site / mySite / shared / Documents / Consultation / Opinion s / 2014 / 14-02-20_EU_US_rebuliding_trust_ES.pdf.

[32] Ver también el Reglamento (CE) Nº 45/2001 del Parlamento Europeo y del Consejo, Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las instituciones y órganos comunitarios y sobre la libre circulación de dichos datos, DO L 8 de 12.1.2001, p. 1, que establece condiciones y salvaguardias detalladas para garantizar el tratamiento legal de los datos personales y, en particular, su artículo 28, apartado 2, 2.

[33] Ver https://www.coe.int/t/dg3/healthbioethic/cometh/ege/20091118%20finalSB%20_2_%20MP.pdf.

[34] Ver http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp231_en.pdf. El 6 de mayo de 2014, la DG Empresa e Industria de la Comisión Europea dirigió una carta al Grupo citado invitando a las autoridades de protección de datos a emitir "recomendaciones sobre cómo abordar las cuestiones de privacidad y protección de datos a nivel europeo y qué acciones deberían emprender para respaldar el establecimiento de un marco adecuado". Este dictamen responde al llamamiento de la Comisión Europea para proporcionar indicaciones prácticas a legisladores y reguladores (tanto en el nivel europeo como nacional, incluidas las Autoridades de Aviación Civil, la industria, los responsables políticos y el público en general. Si bien la Comisión Europea centra su atención en los drones aéreos pilotados a distancia, este dictamen no diferencia entre sistemas de aeronaves no tripuladas totalmente autónomas y no autónomas, teniendo en cuenta que este aspecto no es relevante en relación con los problemas de protección de datos derivados del uso de este tipo de tecnología.

[35] Ver SARMIENTO RAMÍREZ-ESCUDERO, D: *"El "soft law" administrativo: un estudio de los efectos jurídicos de las normas no vinculantes de la Administración",* Cizur Menor, Navarra, Thomson Civitas, 2008.

[36] Ver, en particular, artículos 3, 9 y 13. En el anexo a su Declaración sobre las discusiones actuales sobre el paquete de reforma de protección de datos, el Grupo de Trabajo del artículo 29 propuso una serie de criterios para ayudar a determinar si un tratamiento se realiza o no para uso personal. Ver Propuestas para las enmiendas relativas a la exención para actividades personales o domésticas, disponible en http://ec.europa.eu/justice/data-protection/article-29/documentation/otherdocument/files/2013/20130227_statement_dp_annex2_en.pdf.

[37] Ver sentencia Bodil Lindqvist citada, apartado 47. Ver también la sentencia del TJUE de 11 de diciembre de 2014, As C-212/13, František Ryneš v Úřad pro ochranu osobních údajů, apartado. 33. El TJUE ha declarado que "the application of Directive 95/46 makes it possible, where appropriate, to take into account — in accordance, in particular, with Articles 7(f), 11(2), and 13(1)(d) and (g) of that directive — legitimate interests pursued by the controller, such as the protection of the property, health and life of his family and himself".

[38] Sobre el contenido del derecho a la información en general y su conexión con los restantes derechos fundamentales nos remitimos al excelente trabajo de DOMÉNECH, G, citado más atrás.

[39] ESCRIBANO TORTAJADA, P, op.cit, p.252, cita como ejemplo en el que la captación de una imagen de una persona no se consideraría intromisión ilegítima, el de un reportaje informativo realizado a través de un dron de un acto político en el que se captase al personaje público y al ciudadano que pudiera salir de forma accesoria.

[40] La Directiva 46/95/CE dedicaba su artículo 9 al tratamiento de datos personales y libertad de expresión (ver también su considerando 17), disponiendo lo siguiente: "En lo referente al tratamiento de datos personales con fines exclusivamente periodísticos o de expresión artística o literaria, los Estados miembros establecerán, respecto de las disposiciones del presente capítulo (sobre la licitud del tratamiento de datos personales), del capítulo IV (sobre transferencia de datos personales a terceros países) y del capítulo VI (relativo a la autoridad de control y al Grupo de trabajo sobre la protección de datos personales), exenciones y excepciones sólo en la medida en que resulten necesarias para conciliar el derecho a la intimidad con las normas que rigen la libertad de expresión". En la actualidad la cuestión se regula en el artículo 85 del Reglamento 2016/679 (Tratamiento y libertad de expresión y de información), el cual dispone lo siguiente: "1. Los Estados miembros conciliarán por ley el derecho a la protección de los datos personales en virtud del presente Reglamento con el derecho a la libertad de expresión y de información, incluido el tratamiento con fines periodísticos y fines de expresión académica, artística o literaria. 2. Para el tratamiento realizado con fines periodísticos o con fines de expresión académica, artística o literaria, los Estados miembros establecerán exenciones o excepciones de lo dispuesto en los capítulos II (principios), III (derechos del interesado), IV (responsable y encargado del tratamiento), V (transferencia de datos personales a terceros

países u organizaciones internacionales), VI (autoridades de control independientes), VII (cooperación y coherencia) y IX (disposiciones relativas a situaciones específicas de tratamiento de datos), si son necesarias para conciliar el derecho a la protección de los datos personales con la libertad de expresión e información. 3. Cada Estado miembro notificará a la Comisión las disposiciones legislativas que adopte de conformidad con el apartado 2 y, sin dilación, cualquier modificación posterior, legislativa u otra, de las mismas". Una actividad podría clasificarse como periodística en la medida en que su "objeto es la divulgación al público de información, opiniones o ideas, independientemente del medio que se utilice para transmitirlas". No se limitan a las iniciativas de los medios de comunicación y pueden realizarse con ánimo de lucro "(Ver sentencia del TJUE de 16 de diciembre de 2008, As C-73/07, Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy y Satamedia Oy, párrafo 61). Del mismo modo, el Tribunal Europeo de Derechos Humanos (en adelante TEDH) consideró que "la función de la prensa incluye la creación de foros para el debate público. Sin embargo, la realización de esta función no se limita a los medios de comunicación o periodistas profesionales "(ver sentencia del TEDH Társaság a Szabadságjogokért c. Hungría, de 14 de abril de 2009, apartado 27).

[41] En este sentido, por ejemplo, la adopción de un código de conducta para fines periodísticos podría ser aconsejable para abordar esta cuestión teniendo en cuenta todos los diferentes intereses en juego.

[42] Ver sentencias del TEDH Von Hannover c. Alemania (n. 2), de 7 de Febrero de 2012, apartado 95, Airey c. Irlanda, de 9 de Octubre de 1979, apartado. 32 y Marckx, de 13 de Junio de 1979, apartado. 31.

[43] Se pone como ejemplos que no debería ser posible seguir usando imágenes de tierras agrícolas, tomadas para asegurarse que los plaguicidas se diseminan correctamente con el fin de registrar datos sobre tierras y técnicas vecinas o filmar un área para asegurarla y luego usar las imágenes o videos para multar a las personas que no pagaron por la entrada a dicha área.

[44] En los casos en que los drones tengan un sistema de reconocimiento de imágenes, se propone implementar un mecanismo que facilite el ejercicio de la objeción del interesado en forma de etiquetas activas o pasivas que comuniquen claramente sus intenciones frente al tratamiento de su imagen. Los dispositivos utilizados como etiquetas visuales tradicionalmente tienen como objetivo mostrar a los fotógrafos que trabajan en conferencias públicas cómo se debe utilizar la imagen de las personas fotografiadas. El mecanismo de uso de etiquetas que señalan el consentimiento de los sujetos de datos para el uso y la publicación de su imagen se describió en el proyecto Offlinetags (ver: http://offlinetags.net/es).

[45] Sin embargo, a la luz de la posible gravedad de la interferencia con la protección de datos y la privacidad de otras personas desencadenadas por el uso de drones, de acuerdo con la sentencia del TJUE en el caso Google España (ver apartado 81), está claro que dicho tratamiento difícilmente puede justificarse simplemente por el interés económico que tiene el controlador en ello.

[46] En relación con las diversas tecnologías que pueden leer electrónicamente y procesar datos biométricos (reconocimiento facial, identificación del comportamiento), se puede encontrar un análisis actualizado y aclaraciones y recomendaciones útiles en el siguiente documento: Article 29 Data Protection Working Party, Opinion 3/2012 on developments in biometric technologies, WP193.

[47] Por ejemplo, cuando se utilizan drones equipados con cámaras de video, los que controlan el aparato pueden usar arreglos técnicos para tratar automáticamente las imágenes mediante borrosidad u otros efectos gráficos, a fin de evitar la recopilación de imágenes de personas identificables cuando no sean necesarias. Ver Article 29 Data Protection Working Party, *Opinion 05/2014 on Anonymisation Techniques*, WP216.

[48] Por ejemplo, en el caso de infraestructuras estratégicas o críticas, podría ser aconsejable ajustar el firmware o soporte lógico inalterable de ingeniería de los drones con el fin de inhibir la recopilación de datos dentro de las zonas de exclusión aérea previamente definidas.

[49] El apartado primero de este precepto dispone: "Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados". Se entiende que el principio de privacidad por diseño es una de las obligaciones clave que debía introducirse en la normativa general sobre protección de datos. Esto tiene que hacerse teniendo en cuenta las especificidades de los drones: en efecto, consisten en un vehículo aéreo, el transportista y una carga útil que puede consistir en un sistema de tratamiento de datos. Ambas partes materiales pueden ser producidas por fabricantes completamente diferentes que pueden no tener en cuenta la combinación resultante y sus capacidades. El SEPD ha apoyado la aplicación de este principio, señalando que la Comisión debería recomendar a los fabricantes de drones que: 1º) propongan diferentes categorías de sensores según el objetivo comercial de los compradores del sector privado, para que se pueda elegir el que menos afecte a la privacidad (por ejemplo, un dron utilizado para construir mapas de ruta precisos probablemente no se necesita una cámara de alta resolución capaz de discernir matrículas de vehículos); 2º) configuren la retención de datos por diseño, es decir, la posibilidad de programar la eliminación automática y regular de los datos procesados; 3º) proporcionen herramientas con funciones de protección de datos tales como la posibilidad de encender y apagar sensores en vuelo (para que la grabación no sea continua sino que se active solo cuando sea necesario y proporcional al propósito perseguido), enmascaramiento automático de áreas privadas, detección automática y pixelación de rostros que se juntan accidentalmente en imágenes y videos; 4º) apliquen de manera predeterminada cualquier funcionalidad proporcionada por los dispositivos a la configuración más respetuosa con la privacidad; 5º) proporcionen información clara al usuario sobre cuestiones de privacidad que puedan surgir al usar el dispositivo, posiblemente con un aviso de privacidad que acompañe a todos los drones vendidos dentro del territorio de la UE.

[50] El apartado segundo de este precepto dispone: "El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas". Por ejemplo, los drones desplegados para la entrega de un paquete no deberían estar equipados con cámaras que permitan el reconocimiento facial o la grabación de audio. Tampoco se debería requerir que un dispositivo utilizado para controlar un tejado afectado por daños producidos por una tormenta grabe metraje de todo el vuelo, especialmente si una ubicación de interés se encuentra a cierta distancia del lugar de despegue y aterrizaje. Los mecanismos para garantizar que, por defecto, solo se procesen los datos personales que son necesarios para cada fin específico del procesamiento y que los datos no se recopilan o retienen especialmente más allá del mínimo necesario para esos fines están contemplados en la Propuesta de Reglamento de la Comisión Europea. del Parlamento Europeo y del Consejo sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de dichos datos, COM (2012) 11 final (véase, a este respecto, el artículo 23).

[51] A este respecto, véase, por ejemplo, el Reglamento italiano sobre vehículos aéreos pilotados a distancia (artículo 23).

[52] El artículo 35.1 del Reglamento 2016/679 dispone que: "Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del

tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares".

[53] Al hacer la evaluación se sugiere: 1º) Definir un propósito para su uso con el fin de evitar los riesgos potenciales y recopilar solo los datos estrictamente necesarios para este fin, en línea con el principio de minimización de datos; 2º) Elegir la herramienta adecuada para el trabajo, es decir, no operar drones sobrecargados con sensores de alta resolución si no son necesarios para cumplir los objetivos del usuario; 3º) configurar su dispositivo adoptando el enfoque más respetuoso con la privacidad, es decir, cualquier funcionalidad en el dispositivo debe establecerse en los parámetros más estrictos que satisfagan las necesidades del usuario y afecten menos a la privacidad (por ejemplo, períodos de retención cortos, enmascaramiento de áreas privadas, pixelación de rostros que se acumulan accidentalmente en imágenes y videos, sensores activados solo cuando es necesario).

[54] En este contexto, antes que nada, para cada tipo de aplicación de drones, una evaluación previa debería tener en cuenta los tipos de datos necesarios / estándar que podrían recogerse. Por ejemplo, la simple recopilación de datos relacionados con el vuelo del dron (como altitud, velocidad, duración del vuelo) puede no desencadenar inmediatamente la aplicación de las obligaciones de protección de datos, a menos que el piloto u otro individuo sean identificables a partir de los datos (por ejemplo el nombre del piloto o el número de empleado se incluye dentro de los metadatos del registro).

[55] Véase CLARKE, R: "Regulación del impacto de los aviones no tripulados civiles en la privacidad del comportamiento", *Computer Law & Security Review* 30, 3 de junio de 2014.

[56] Se ha advertido que es de suma importancia que el responsable del tratamiento y el encargado del tratamiento deben estar claramente identificados para cada tipo de operación con drones, especialmente mediante la evaluación de los elementos esenciales para distinguir al responsable de otros actores. Por ejemplo, aunque este rol podría estar claro cuando el dron es utilizado directamente por una empresa que lo compró para entregar paquetes, cosa distinta es el caso de una empresa que realice un mapa de un área para un operador de drones (donde hay que distinguir dos figuras). En el dictamen 1/2010 del Grupo de Trabajo del artículo 29 (Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", WP169) se puede encontrar una guía clara para identificar las diferentes combinaciones de responsabilidades entre las diferentes entidades involucradas en un tratamiento conjunto. En el artículo 4 del **Reglamento (UE) 2016/679, se recoge en su punto** 7º) el «responsable del tratamiento» o «responsable», definido como la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros. En su apartado 8º) se define el «encargado del tratamiento» o «encargado» como la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

[57] MUÑOZ, T, op.cit, explica que "una de las principales dificultades resulta de la obligación del deber de informar a las personas sujetas a las actividades de aviones no tripulados. Teóricamente, bajo las leyes de la UE y de los Estados miembros, los controladores de aviones no tripulados han de proporcionar a los afectados información sobre el tratamiento de sus datos de carácter personal. El límite es que ello exija esfuerzos desproporcionados, excepción que les beneficiará. Advierte que "con relación a los drones ciertas obligaciones en materia de requisitos de información serían difíciles de cumplir". Apunta que el uso de los drones no está previsto en la Ley de Protección de Datos española.

[58] Si, por ejemplo, las personas asisten a un evento al aire libre, es fácilmente concebible informar de la presencia del dron a través de paneles de aviso de privacidad ubicados en la entrada de su zona de vuelo.

[59] Por ejemplo, si es un evento deportivo avisando en un programa de deportes.

[60] Por ejemplo, un agente inmobiliario, que utiliza un dron para grabar imágenes de una propiedad en venta, podría escribir a los vecinos con anticipación, pero también visitar a las propiedades cercanas el día de la grabación y alertarlas sobre el tratamiento.

[61] Dicha información podría darse de forma general explicando que la infraestructura está siendo sobrevolada por un dron, sin necesidad de dar detalles sobre concretos vuelos futuros. En este ámbito también hay que hacer referencia a problemas de seguridad relevantes que se pueden plantear en algunos supuestos. Y es que existen documentadas noticias sobre vuelos ilegales de drones sobre edificios estratégicos de áreas urbanas sin ninguna posibilidad de identificar a las personas que los operaban.

[62] La tarea de mantener este recurso (que podría ser un sitio web específico donde los drones podrían rastrearse con antelación, y / o un registro central de acceso público) podría confiarse, por ejemplo, a la EASA o a las autoridades nacionales de aviación o de protección de datos. La obligación de informar no solo cubriría los vuelos planificados, sino también el propósito de tratar datos personales. Igualmente debe recordarse que, de todos modos, en la mayoría de los casos las autoridades nacionales deben estar informadas sobre cualquier actividad de drones.

[63] Ver Working Group on Data Protection in Telecommunication, *Working paper on Privacy and Aerial Surveillance*, 54th meeting, Berlin, September 2013, published at www.berlin-privacy-group.org

[64] MUÑOZ, T op.cit, apunta que *"las imágenes obtenidas por entidades privadas deben cumplir con el principio de calidad de los datos y evitar todas las imágenes innecesarias de los espacios públicos.* En el caso de uso de drones en espacios cerrados, esta información podría facilitarse en el mismo momento en que se solicita el consentimiento de los afectados o mediante la exposición de carteles informativos. En el caso de uso de drones en espacios abiertos delimitados, la información también podría facilitarse mediante la colocación de estos carteles informativos. En caso de espacios abiertos no delimitados, el responsable podría plantear ante la Agencia de Protección de Datos, a la vista de las circunstancias concretas de cada caso, si las medidas que pretende adoptar para facilitar a los interesados la información relativa al ejercicio de los derechos ARCO se adecuan a la normativa de protección de datos".

[65] Con todo, esta recomendación plantea problemas. Así se advierte que, por ejemplo, si una farmacia realiza entregas regulares por drones a la propiedad de una persona, se puede deducir que el ocupante sufre un problema médico grave. Requerir que un individuo presente planes de vuelo de drones o que brinde la posibilidad de consultar los vuelos históricos de un usuario u organización de drones individual, incluidos los sitios de despegue y aterrizaje, es probable que genere preocupaciones importantes de protección de datos.

[66] Realizados por las autoridades competentes que los fabricantes pueden indicar, por ejemplo, mediante remisión con un enlace a un recurso de información administrado por dichas autoridades.

[67] Ver artículos 32 y ss del Reglamento 2016/679.

[68] Por ejemplo, las imágenes / videos capturados por drones con el propósito de asegurar el área al aire libre de un festival solo se deberían conservar durante el tiempo necesario para investigar posibles reclamaciones o problemas relacionados con la seguridad.

[69] En relación con todos estos aspectos, el Grupo de Trabajo del artículo 29 desea llamar la atención de los controladores de datos, al menos, con respecto a lo siguiente: a) Se debe permitir que un número limitado de personas autorizadas, para ser especificadas, vea o acceda a las imágenes grabadas. b) Se debe otorgar acceso limitado a las personas antes mencionadas, según la necesidad de saber c) el almacenamiento debe ser cifrado y la transmisión de información debe producirse cuando sea necesario d) deben existir registros de todas las instancias de acceso y uso de material grabado e) deben establecerse períodos de almacenamiento de datos estrictos y garantizarse la eliminación o anonimización automática una vez que el período de almacenamiento de datos ha expirado f) se debe garantizar la notificación de la existencia de una violación de datos a la autoridad de protección de datos (en la medida en que sea legalmente obligatorio).

[70] Por ejemplo, en Alemania, las normas de tráfico aéreo (Luftverkehrs-Ordnung (LuftVO)) se modificaron en 2012 para incluir el cumplimiento de los requisitos de protección de datos como parte de un examen que realizarían las autoridades aeronáuticas competentes de los Estados federales al otorgar los permisos para operar una aeronave. Del mismo modo, el Reglamento sobre vehículos aéreos pilotados a distancia adoptado en Italia el 16 de diciembre de 2013 establece que "cuando las operaciones llevadas a cabo por un dron puedan conducir al tratamiento de datos personales, este hecho debe mencionarse en la documentación presentada para la concesión de la autorización pertinente "(Artículo 22).

[71] En la mayoría de los casos, las CAA otorgan certificaciones o autorizaciones muy específicas que regulan el uso de drones civiles: el área de vuelo y la ruta, el dispositivo.

[72] El artículo 40 del Reglamento 2016/679 dispone que "los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán la elaboración de códigos de conducta destinados a contribuir a la correcta aplicación del presente Reglamento, teniendo en cuenta las características específicas de los distintos sectores de tratamiento y las necesidades específicas de las microempresas y las pequeñas y medianas empresas. 2. Las asociaciones y otros organismos representativos de categorías de responsables o encargados del tratamiento podrán elaborar códigos de conducta o modificar o ampliar dichos códigos con objeto de especificar la aplicación del presente Reglamento […]".

[73] El artículo 42.1 del Reglamento 2016/679 dispone que: "Los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán, en particular a nivel de la Unión, la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos a fin de demostrar el cumplimiento de lo dispuesto en el presente Reglamento en las operaciones de tratamiento de los responsables y los encargados. Se tendrán en cuenta las necesidades específicas de las microempresas y las pequeñas y medianas empresas".

[74] Un ejemplo interesante de folleto sobre el uso personal de drones ("*Règles d'un bon usage d'un drone de loisir*") puede encontrarse en http://www.developpement-durable.gouv.fr/IMG/pdf/Drone-_Notice_securite-2.pdf. También es muy ilustrativa la lista de cosas permitidas y prohibidas en el vuelo de los drones diseñada en EEUU por la FAA publicada en http://www.faa.gov/uas/publications/model_aircraft_operators.

[75] Ver BLASI CASAGRAN, C: "El empleo emergente de drones con fines policiales en la Unión Europea: avances y limitaciones", Julio, 10, 2014, http://www.seguridadinternacional.es/?q=es/content/el-empleo-emergente-de-drones-con-fines-policiales-en-la-unión-europea-avances-y-limitaciones y ELORDI VILLENA, M: "El uso de vehículos aéreos no tripulados (drones) en las labores de seguridad y vigilancia de la Administración (Protección de la intimidad y responsabilidad de las Administraciones Públicas", en Congreso Derecho TICs-SICARM 2014: Innovación, tecnología y gestión avanzada de la información administrativa. Implicaciones jurídicas del cambio de paradigma.

[76] ESCRIBANO TORTAJADA, P, op.cit, p.252 y ss, nos recuerda que nuestro Tribunal Supremo se ha hecho del problema que plantean los drones en su sentencia de la Sala de lo Penal de 20 de abril, nº 329/2016, referida a unos agentes de policía que habían observado en el interior de una vivienda con unos prismáticos.

[77] Ver sentencia Rundfunk, As Ac C-465/00 C-138/01 y C-139/01, apartados 72 y 91.

[78] Ver sentencia Marguerite Johnston contra Chief Constable of Royal Ulster Constabulary, As C-222/84. De este modo, las actividades de los organismos de inteligencia que entren dentro del ámbito de la legislación de la UE (por ejemplo, vigilancia de la política exterior, aplicación de la ley o fines puramente comerciales) deben respetar estos principios. Véase también el dictamen del SEPD de 20 de febrero de 2014 sobre la Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre «Reconstrucción de la confianza en los flujos de datos UE-EE. UU.»

[79] El TEDH aplicó estos requisitos a la interferencia de las autoridades policiales con el ejercicio del derecho a la privacidad en su sentencia de la Gran Sala del TEDH de 4 de diciembre de 2008, S. y Marper c. Reino Unido, nº 30562/04 y 30566/04,

[80] Si los drones se utilizan en el marco de la cooperación policial y judicial en materia penal, cualquier intercambio entre los Estados miembros de datos personales recopilados a través de drones deberá cumplir sus requisitos especificados en la Decisión marco 2008/977 / JAI del Consejo 27 de noviembre de 2008, sobre la protección de los datos personales tratados en el marco de la cooperación policial y judicial en materia penal, DO L350, 30.12.2008, p. 60. Véase sin embargo el memorándum explicativo de la Comisión Europea a la Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas con respecto al tratamiento de datos personales por parte de las autoridades competentes a efectos de prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, y la libre circulación de dichos datos / * COM / 2012/010 final - 2012/0010 (COD). En particular, página 2, párrafo 2. Véase igualmente el dictamen 04/2014 sobre la vigilancia de las comunicaciones electrónicas con fines de inteligencia y seguridad nacional, adoptado el 10 de abril de 2014, 819/14 / EN WP 215, página 6 disponible en http://ec.europa.eu/justice/data- protection / article-29 / documentation / opinionrecommendation / files / 2014 / wp215_en.pdf.

[81] Sobre la actividad de vigilancia que implica una nueva operación de tratamiento, se apunta la necesidad de una autorización de la actividad de un juez u otra autoridad independiente ya que reduciría el riesgo de abuso al garantizar que la necesidad y la proporcionalidad se determinen en el momento en que se toman las decisiones que afectan la vida privada de los ciudadanos. La autorización debe contener una evaluación de la necesidad y proporcionalidad de la medida, establecer las salvaguardias apropiadas cuando sea necesario y estar limitada en el tiempo.

[82] El uso de drones para la aplicación de la ley, incluso en el caso de investigaciones justificadas, como una vigilancia específica, debería exigir un régimen de aprobación más elevado en la jerarquía de la organización.

[83] A este respecto, el Grupo de Trabajo del artículo 29 llama la atención sobre su Dictamen 01/2014 sobre la aplicación de conceptos de necesidad y proporcionalidad y protección de datos dentro del sector de la aplicación de la ley.