

**EL USO EMERGENTE DE DRONES
CIVILES EN ESPAÑA. ESTATUTO
JURÍDICO E IMPACTO EN EL DERECHO
A LA PROTECCIÓN DE DATOS**

CRISTINA PAUNER CHULVI

SUMARIO

1. LA REVOLUCIÓN DE LOS DRONES. 2. EL MARCO REGULATORIO ESPAÑOL EN MATERIA DE DRONES. 2.1 Algunas notas aclaratorias sobre el concepto de dron. 2.2 Los usos civiles de los drones. 3. EL IMPACTO DEL USO CIVIL DE LOS DRONES EN LA PROTECCIÓN DE LOS DATOS DE CARÁCTER PERSONAL. 3.1 El tratamiento legal de la protección de datos en los usos de drones para fines públicos. 3.2 El cumplimiento de los principios de la LOPD por el operador de un dron para fines privados. 4. PROPUESTAS PARA UN MARCO REGULADOR ARMONIZADO EN RELACIÓN CON LA PROTECCIÓN DE DATOS Y LAS OPERACIONES DE DRONES CIVILES. 5. REFLEXIONES FINALES.

Fecha recepción: 14.10.2015
Fecha aceptación: 19.01.2016

EL USO EMERGENTE DE DRONES CIVILES EN ESPAÑA. ESTATUTO JURÍDICO E IMPACTO EN EL DERECHO A LA PROTECCIÓN DE DATOS*

CRISTINA PAUNER CHULVI¹

Profesora Titular de Derecho Constitucional

1. LA REVOLUCIÓN DE LOS DRONES

Los drones² están protagonizando una revolución en el sector de la aviación y, sin abandonar su empleo en el campo militar donde siguen utilizándose ampliamente, han irrumpido con fuerza en el mercado mundial ofreciendo múltiples aplicaciones para uso civil³. De manera sintética, un dron es una aeronave pilotada por control remoto. Estos vehículos vuelan sin un piloto al mando a

* El presente trabajo se enmarca en el proyecto de investigación CRISP (Esquemas de Evaluación y Certificación para productos de seguridad) financiado por la Comisión Europea (número de subvención 607941) y la ayuda del Programa de Movilidad del Ministerio de Educación, Cultura y Deporte (PRX14/00107).

¹ Departamento de Derecho Público. Área de Derecho Constitucional. Universitat Jaume I. Campus del Riu Sec. E-12071 Castelló de la Plana. Email: pauner@uji.es

² La terminología manejada para denominar a este tipo de aeronaves es muy variada. Si bien su uso más extendido y popularizado es el de RPA (por sus siglas en inglés, Remotely Piloted Aircraft), también se les conoce como UAV (Unmanned Aerial Vehicle) y UAS (Unmanned Aerial System). En el entorno académico, se sigue empleando con frecuencia la expresión «drones» que es la que utilizaremos en nuestro trabajo.

³ El uso militar de los drones no es abordado en el presente estudio. Su regulación se contiene en la Orden PRE/1366/2010, de 20 de mayo, por la que se modifica el Reglamento de la Circulación Aérea Operativa, aprobado por el Real Decreto 1489/1994, de 1 de julio.

bordo y se controlan a distancia desde otro lugar (tierra, espacio u otra aeronave). Existe una amplia variedad de prototipos que pueden ir equipados con tecnología muy heterogénea, desde sencillos dispositivos como cámaras o sensores hasta instrumentos muy perfeccionados y complejos como objetivos zoom de alta potencia, visión nocturna, infrarrojos, imágenes térmicas, tecnologías de radar, vídeo de reconocimiento biométrico facial, etc.

Esta versatilidad de capacidades permite que los drones puedan aplicarse a múltiples tareas para fines profesionales, comerciales o recreativos y que sean considerados como una tecnología puntera y emergente con un enorme potencial económico en todo el mundo⁴ por lo que se están invirtiendo muchos esfuerzos en desarrollar un marco legal que regule su uso civil.

A nivel nacional, son varios los países del entorno europeo que ya han aprobado alguna reglamentación que cubre las operaciones civiles que se llevan a cabo con drones⁵. Según Eurocontrol⁶, existen normativas sobre aeronaves civiles pilotadas por control remoto en Alemania, Austria, Bélgica, Croacia, Dinamarca, Finlandia, Francia, Irlanda, Italia, Holanda, Reino Unido, República Checa, Suecia y Suiza. España también cuenta con regulación desde julio de 2014 aunque se trata de normativa temporal por lo que el Ejecutivo español está preparando una nueva legislación que amplía las posibilidades de uso de estos vehículos y cuya aprobación se espera con carácter inminente.

⁴ Según cálculos de la Comisión Europea, en 2050 este sector habrá generado 150.000 empleos y obtendrá alrededor de 15.000 millones de euros al año de beneficios mientras que la Administración Federal de Aviación de Estados Unidos (FAA) considera que el mercado de los drones domésticos podrá generar unos 90.000 millones de dólares en la próxima década.

⁵ La Agencia Europea de Seguridad Aérea (EASA) tiene competencia para regular los drones de más de 150 kilos de masa al despegue dejando en manos de las autoridades aeronáuticas de los distintos Estados miembros la reglamentación de los drones de peso inferior, los vuelos experimentales, los vuelos gubernamentales militares y no militares y los aeromodelos [Reglamento (CE) no 216/2008]. No obstante, esta división se ha revelado disfuncional al complicar el avance de una regulación coherente y exhaustiva para Europa por lo que las instituciones europeas abogan por la eliminación del umbral de 150 kilos y la transferencia de las competencias sobre toda clase de drones a la Unión Europea sin atención a su peso [Parlamento Europeo, *Resolución del Parlamento Europeo sobre el uso seguro de los sistemas de aeronaves pilotadas de forma remota (RPAS), comúnmente conocidos como vehículos aéreos no tripulados (UAV), en el ámbito de la aviación civil*, de 29 de octubre de 2015, <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2015-0390+0+DOC+PDF+V0//ES>].

⁶ La Organización Europea para la Seguridad de la Navegación Aérea, Eurocontrol, es una organización intergubernamental compuesta por 41 Estados que tiene como objetivo el desarrollo de un sistema seguro, eficaz y coordinado del tráfico aéreo europeo. El listado de normativas nacionales sobre drones puede consultarse en <https://easa.europa.eu/unmanned-aircraft-systems-uas-and-remotely-piloted-aircraft-systems-rpas>.

También en Europa se trabaja intensamente para elaborar un marco regulador común y armonizador para las operaciones civiles de drones⁷. El objetivo es acabar con las diferencias y lagunas contenidas en las normativas nacionales para garantizar que estos dispositivos no tripulados no representan ninguna amenaza para la seguridad pública y la privacidad de los ciudadanos.

Desde las primeras iniciativas surgidas para regular este sector, la prioridad de las autoridades de aviación en todo el mundo ha sido la de conseguir un nivel de seguridad equivalente al de las operaciones que se realizan con aparatos tripulados. En los últimos años, sin embargo, se ha dado paso a un perceptible movimiento normativo centrado en la defensa de otros derechos fundamentales de los ciudadanos, señaladamente, la protección de datos y la intimidad. El empleo creciente de drones por las Fuerzas y Cuerpos de seguridad estatales y su masiva utilización por el sector privado —ciudadanos, profesionales y empresas— ha tenido mucho que ver en esa mayor preocupación por los aspectos relacionados con la privacidad. De hecho, la transformación de los drones en una tecnología de moda así como la reducción del precio de estos aparatos —se puede conseguir un modelo básico a partir de unos 60 €— han popularizado su uso y se prevé su rápida conversión en artículos de consumo masivo, básicamente con fines comerciales, profesionales, deportivos o recreativos.

Los ejemplos de esta nueva orientación se detectan a nivel mundial, tanto en el entorno europeo como norteamericano. Así, en Estados Unidos, el pasado 4 de marzo de 2015, el Departamento Nacional de Comercio, Telecomunicaciones e Información Administrativa (NTIA) anunció que está buscando aportaciones sobre la privacidad, la transparencia y las cuestiones de responsabilidad en relación con el uso comercial y privado de los sistemas de aeronaves no tripuladas⁸.

⁷ La Comisión Europea comenzó a desplegar políticas sobre drones en la última década aunque el empuje definitivo se da a partir de 2012 con la vista puesta en el año 2016 para culminar la labor normativa de la integración de los drones en el espacio aéreo europeo. El primer texto a destacar fue el Documento de Trabajo de la Comisión Europea, *Hacia una estrategia europea para el desarrollo de las aplicaciones civiles de las aeronaves no tripuladas (RPAS)*, de septiembre de 2012, seguido de la *Hoja de Ruta para la Integración de aeronaves civiles controladas por control remoto en el sistema europeo de aviación* elaborada por el Grupo Directivo Europeo sobre drones en junio de 2013 hasta llegar a la decisiva Comunicación de la Comisión Europea sobre *Una nueva era de la aviación. Abrir el mercado de la aviación al uso civil de sistemas de aeronaves pilotadas de forma remota de manera segura y sostenible*, de abril de 2014, que presenta la estrategia de la Comisión para impulsar el desarrollo del mercado europeo de drones.

⁸ Department of Commerce, National Telecommunications and Information Administration, *Privacy, Transparency and Accountability Regarding Commercial and Private Use of Unmanned Aircraft Systems*, https://www.ntia.doc.gov/files/ntia/publications/rfc_uas_privacy_03052015.pdf

El anuncio de la NTIA se produjo en respuesta a un Memorando Presidencial⁹ emitido el 15 de febrero para iniciar ese proceso de consultas con todos los sectores interesados y en el que, explícitamente, se subraya la necesidad de abordar los retos que los drones plantean para la privacidad.

En Europa, por su parte, se ha dado un paso definitivo con la adopción de la *Resolución del Parlamento Europeo*, de 29 de octubre de 2015, *sobre el uso seguro de los sistemas de aeronaves pilotadas de forma remota (RPAS) en el ámbito de la aviación civil*¹⁰ que abre la puerta a los usos de drones civiles con fines comerciales y profesionales exigiendo la incorporación de garantías relativas a la protección de la vida privada y de los datos personales. Esta resolución permitirá crear un marco legislativo común que garantice que todas las partes implicadas realizan un tratamiento adecuado de los datos que se ajuste a los principios de transparencia, necesidad, proporcionalidad y oportuna cancelación en el tratamiento de los mismos en cumplimiento de la normativa europea de protección de datos.

El objetivo de este estudio es presentar el marco regulatorio español del uso de los drones en el ámbito civil comenzando por un análisis del concepto de dron y de las condiciones bajo las que deben operar estas aeronaves para centrarnos en la exposición de los retos que su utilización plantea para la intimidad y la protección de datos de los ciudadanos. Se estudiará la cobertura que actualmente ofrece la normativa europea y española en materia de protección de datos y a la que habrá de ajustarse la obtención y el tratamiento de datos personales captados mediante la utilización de drones. En la parte final de este trabajo se expondrán algunas propuestas de solución surgidas en el entorno europeo para afrontar los mencionados retos.

2. EL MARCO REGULATORIO ESPAÑOL EN MATERIA DE DRONES

2.1 *Algunas notas aclaratorias sobre el concepto de dron*

El 4 de julio de 2014, el Gobierno español aprobó el Real Decreto-ley 8/2014 de aprobación de medidas urgentes para el crecimiento, la competitividad y la

⁹ The White House, *Presidential Memorandum: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights and Civil Liberties in Domestic Use of Unmanned Aircrafts Systems*, Febrero de 2015. <https://www.whitehouse.gov/the-press-office/2015/02/15/presidential-memorandum-promoting-economic-competitiveness-while-safegua>

¹⁰ Parlamento Europeo, *Resolución sobre el uso seguro de los sistemas de aeronaves pilotadas de forma remota (RPAS) en el ámbito de la aviación civil*, cit.

eficiencia¹¹ en cuyo artículo 50 se adoptaban las medidas temporales para operaciones de aeronaves civiles pilotadas por control remoto. El Real Decreto se convirtió en la Ley 18/2014, de 15 de octubre¹², que fue adoptada con una vigencia temporal hasta que el Gobierno determine reglamentariamente el nuevo régimen jurídico aplicable a estas aeronaves, labor legislativa que se encuentra en fase muy avanzada en el momento de redactar estas líneas. El régimen normativo español sobre drones se completa con lo dispuesto en la Ley 48/1960, de 21 de julio, de Navegación Aérea (LNA) que se modificó para establecer con carácter concluyente que estos artefactos son efectivamente aeronaves y como tales su utilización civil está sujeta a la legislación aeronáutica civil¹³.

Ninguna de las dos leyes mencionadas contiene una definición de dron aunque sí lo hace el borrador de Real Decreto proyectado. A los efectos del futuro Real Decreto se entiende por «Aeronave pilotada por control remoto (RPA)» aquella aeronave no tripulada, pilotada a distancia desde una estación de pilotaje remoto y por «Sistema de aeronave pilotada por control remoto (RPAS)» el conjunto de elementos configurables integrado por una aeronave pilotada por control remoto (RPA), su estación o estaciones de pilotaje remoto conexas, los necesarios enlaces de mando y control y cualquier otro elemento de sistema que pueda requerirse en cualquier momento durante la operación de vuelo. En atención a estas descripciones, no se incluye en la definición de dron la aeronave no tripulada y plenamente autónoma, esto es, aquella que está controlada por un programa de vuelo automático. Lo definitivo para ser calificado como dron, por tanto, es que se trate de una aeronave no tripulada y *pilotada a distancia*¹⁴.

¹¹ Un detallado análisis del contenido del RD 8/2014 en GUERRERO LEBRÓN, M. J., «La regulación transitoria de los operadores de aeronaves civiles pilotadas por control remoto», *La Ley mercantil*, 31 de julio de 2014, Editorial La Ley.

¹² Ley 18/2014, de 15 de octubre, de aprobación de medidas urgentes para el crecimiento, la competitividad y la eficiencia, *BOE* núm. 252, de 17 de octubre de 2014.

¹³ Según el artículo 11 LNA «Se entiende por aeronave: a) Toda construcción apta para el transporte de personas o cosas capaz de moverse en la atmósfera merced a las reacciones del aire, sea o no más ligera que este y tenga o no órganos motopropulsores. b) Cualquier máquina pilotada por control remoto que pueda sustentarse en la atmósfera por reacciones del aire que no sean las reacciones del mismo contra la superficie de la tierra» (Artículo 11 redactado por el apartado uno del artículo 51 de la Ley 18/2014, de 15 de octubre, de aprobación de medidas urgentes para el crecimiento, la competitividad y la eficiencia).

¹⁴ En coherencia con la terminología internacional y europea, las etiquetas de «aeronave no tripulada» o «sistema de aeronave no tripulada» se emplean como términos globales mientras que «aeronave pilotada por control remoto» (o a distancia) se refiere solamente al subconjunto de aeronaves no tripuladas [Párrafo 3.3 de la Circular 328 OACI y Comisión Europea, Comunicación de la Comisión al Parlamento Europeo y al Consejo, *Una nueva era de la aviación. Abrir el mercado*

En lo que se refiere a las características de los drones, la Ley 18/2014 establece requisitos sobre el peso máximo del aparato al despegue y clasifica los aviones en tres categorías en función de su peso siempre que se trate, como avanzábamos unas líneas más arriba, de aeronaves pilotadas por control remoto de peso inferior a los 150 kilos¹⁵. Independientemente del peso hay algunos requisitos comunes para todos los tipos de aeronaves. En primer lugar, es imprescindible contar con un carnet de piloto de drones para poder operar en España —un certificado básico para volar dentro del alcance visual del piloto o certificado avanzado para volar más allá del alcance visual del piloto—. En segundo término, toda aeronave civil dirigida por control remoto deberá estar provista de una placa de identificación de la aeronave y de los datos de la empresa operadora. Estos datos de identificación son muy relevantes a la hora de determinar el sujeto responsable de las actividades que desarrolle un dron y sus consecuencias. Piénsese, por ejemplo, en el supuesto de los daños ocasionados por el vuelo del aparato en bienes y/o personas o la determinación, en su caso, del responsable del tratamiento de los datos capturados y de las obligaciones de custodia y conservación de datos y ficheros. En tercer lugar, todas las empresas operadoras deben tener un manual de operaciones, un estudio aeronáutico de seguridad para cada operación, un programa de mantenimiento de la aeronave de acuerdo con las recomendaciones del fabricante y un seguro de vuelo según la normativa vigente.

2.2 *Los usos civiles de los drones*

En atención al régimen legislativo aplicable en España podemos diferenciar dos categorías de drones para usos civiles, a saber, los de uso profesional y/o comercial y los de uso recreativo.

de la aviación al uso civil de sistemas de aeronaves pilotadas de forma remota de manera segura y sostenible, de 8 de abril de 2014, COM(2014)207}.

¹⁵ La Ley distingue entre 1. Drones de más de 25 kilos que no superan los 150 kilos: son las únicas aeronaves que deberán estar registradas en el Registro de Matrícula de Aeronaves y contar con un certificado de aeronavegabilidad emitido por la Agencia Estatal de Seguridad Aérea (AESA). El piloto necesitará un certificado básico o avanzado emitido por una organización de formación autorizada. 2. Drones de menos de 25 kilos y hasta 2 kilos: no necesitan estar inscritos en el registro de aeronaves ni disponer de un certificado de aeronavegabilidad pero deberán emitir una comunicación previa de vuelo así como una declaración responsable a la AESA con una antelación mínima de cinco días. El dron debe estar dentro del alcance visual del piloto y se requiere un permiso especial para la obtención de fotografías o filmaciones. 3. Drones inferiores a 2 kilos: son los únicos que pueden volar más allá del alcance visual del piloto pero sujetos al alcance de la emisión por radio de la estación de control. Aunque tampoco se exige certificado ni inscripción, debe emitirse un aviso de vuelo al resto de usuarios del espacio aéreo informando del lugar y hora en los que se volará.

a) Uso profesional y comercial

La Ley 18/2014 fija los requisitos de explotación de estas aeronaves para la realización de trabajos científicos o técnicos (artículo 50.3), vuelos de prueba de producción y de mantenimiento, vuelos de demostración no abiertos al público, vuelos para programas de investigación en los que se trate de demostrar la viabilidad de realizar determinada actividad con aeronaves civiles pilotadas por control remoto, vuelos de desarrollo de nuevos productos o para demostrar la seguridad de las operaciones específicas de trabajos técnicos o científicos (artículo 50.4). Partiendo de este listado, podemos concretar las actividades aéreas que la regulación española permite a los aviones no tripulados tales como: actividades de investigación y desarrollo; tratamientos aéreos, pesticidas y otros tratamientos que implican la difusión de sustancias en el suelo o la atmósfera, incluidas las actividades de lucha contra el fuego; observación y actividades de vigilancia aérea, incluyendo la filmación y el seguimiento de los incendios forestales; publicidad, emisiones aéreas de radio y televisión y de emergencia, operaciones de búsqueda y rescate, así como otras obras especiales.

Estas actividades podrán realizarse de forma comercial o no pero el mercado para las aeronaves no tripuladas civiles permanecerá limitado ya que, en un primer momento y hasta que no esté aprobada la reglamentación definitiva¹⁶, las operaciones autorizadas se limitan a zonas no pobladas, esto es, siempre en zonas fuera de aglomeraciones de edificios en ciudades, pueblos o lugares habitados o de reuniones de personas al aire libre, de día, en condiciones meteorológicas visuales, a una altura máxima de 120 metros y acotadas al espacio aéreo no controlado¹⁷. Esto significa que, hoy por hoy y en tanto no se apruebe la normativa proyectada, la seguridad que exigen las operaciones realizadas con drones se consigue obligándoles a operar en el espacio aéreo segregado, que es aquel que se reserva para realizar una actividad aérea concreta. Esto se logra estableciendo zonas y pasillos aéreos de uso reservado y exclusivo para los drones. El resto de

¹⁶ Una de las principales novedades que presenta el borrador de Real Decreto que circula actualmente es que autorizará los vuelos de drones en ciudades siempre que pesen menos de 10 kilos, sin alejarse más de 100 metros del piloto ni superar los 120 metros de altura y sólo podrán ser usados en zonas acotadas o a una distancia de seguridad de edificios o personas contando con los permisos correspondientes.

¹⁷ La OACI divide al espacio aéreo en siete partes, nombradas con una letra de la A a la G. La clase A es el sector con el nivel más alto de control, mientras que la clase G refiere al espacio aéreo no controlado. Cada calificación indica las normas operativas, el equipamiento mínimo y los requisitos que los pilotos deben respetar para poder volar.

aeronaves no podrán hacer uso de ese espacio aéreo segregado ni el dron operar fuera de este¹⁸.

Por último, la Ley 18/2014, orientada exclusivamente a favorecer el desarrollo en condiciones de *seguridad* de este sector, establece que el cumplimiento de lo dispuesto en el artículo 50 «no exime al operador, que es, en todo caso, el responsable de la aeronave y de la operación, del cumplimiento del resto de la normativa aplicable, en particular en relación con el uso del espectro radioeléctrico, la protección de datos o la toma de imágenes aéreas, ni de su responsabilidad por los daños causados por la operación o la aeronave» (artículo 50.1). Concretamente, la protección de la intimidad y la protección de los datos de carácter personal obliga al operador a adoptar las medidas necesarias para garantizar el cumplimiento de lo dispuesto en la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen y en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos (LOPD).

b) Uso recreativo

El régimen de las aeronaves de uso lúdico no se rige por lo dispuesto en la LNA que excluye de su aplicación la operación de aeronaves civiles pilotadas por control remoto «que sean utilizadas exclusivamente con fines recreativos o deportivos» (artículo 150.2), esto es, las demostraciones aéreas, las actividades deportivas, las recreativas o las de competición. Este tipo de dispositivos empleados con fines deportivos o de ocio son considerados aeromodelos pero su catalogación como aeronaves las somete también a la observancia de las leyes aeronáuticas vigentes. El borrador de Real Decreto sí contempla el uso recreativo de estas

¹⁸ Esta solución es a todas luces insuficiente e implica una serie de limitaciones que están frenando el desarrollo y la expansión del sector. Por este motivo son numerosas las iniciativas internacionales y europeas surgidas para regular la integración de los drones en el espacio aéreo controlado y no segregado aunque, por el momento y debido tanto a la complejidad y extensión de las áreas a las que afecta como a la exigencia de alcanzar soluciones internacionalmente aceptadas, no han fructificado en una reglamentación completa y homogénea que unifique las exigencias que estos sistemas deben cumplir para poder operar con un nivel de seguridad equivalente al de las aeronaves tripuladas y compartir el espacio aéreo con la aviación convencional. Un riguroso análisis sobre el régimen legal de los drones y sus posibilidades de integración en el espacio aéreo no segregado en GUERRERO LEBRÓN, M. J., C. CUERNO REJADO y P. MÁRQUEZ LOBILLO, «Aeronaves no tripuladas. Estado de la legislación para realizar su integración en el espacio aéreo no segregado», *Revista del Derecho del Transporte*, núm. 12, 2013, págs. 63 a 106.

aeronaves a las que denomina «aeromodelos radio-controlados» y dispone las reglas de seguridad bajo las que deberán operar¹⁹.

Así las cosas y en primer lugar, la práctica del aeromodelismo está regulada por la Real Federación Aeronáutica de España. Además, debe tenerse en cuenta lo establecido por la legislación propia que cada Comunidad Autónoma y las ordenanzas municipales que cada municipio puede tener sobre esta actividad lúdica o deportiva. Los aeromodelos no necesitan autorización de AESA²⁰ para volar aunque deben hacerlo por debajo de los 100 metros de altura, dentro del alcance visual del operador y en zonas adecuadas para ello como zonas de vuelo de aeromodelismo o zonas despobladas.

En segundo lugar y atendiendo a su catalogación como aeronaves, estos vehículos aéreos no pueden entrar en espacio aéreo controlado sin autorización (por ejemplo, aeropuertos o zonas con espacio aéreo restringido) ni tampoco pueden volarse en espacios aéreos no controlados (por ejemplo, una plaza pública o una reunión de personas al aire libre)²¹.

En tercer lugar, cuando se trate de vuelos practicados en exhibiciones y festivales de carácter aeronáutico debe asegurarse la seguridad de los mismos mediante el cumplimiento de los requisitos aplicables para la realización y autorización de una demostración aérea civil²².

En último lugar y por lo que a nosotros nos interesa, también los usuarios y operadores de drones con fines recreativos o de ocio deben observar lo dispuesto en la Ley Orgánica 1/1982, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen y en la LOPD cuando con

¹⁹ Se trata de las siguientes condiciones: en vuelo diurno y en condiciones meteorológicas de vuelo visual, dentro del alcance visual del piloto, en zonas autorizadas fuera de áreas pobladas, en espacio aéreo no controlado, manteniendo una distancia adecuada a los obstáculos y en zonas fuera de aglomeraciones de edificios en ciudades, pueblos o lugares habitados o sobre una reunión de personas al aire libre. El Real Decreto proyectado no afectará a la utilización de aeromodelos en prácticas deportivas que se regirá por sus disposiciones específicas.

²⁰ A diferencia de Estados Unidos donde el uso lúdico de los drones de entre 250 gramos y 25 kilos ha comenzado a ser controlado mediante un sistema de registro obligatorio impuesto por la FAA desde el pasado 26 de diciembre (*El País*, «Estados Unidos controla la expansión lúdica de los drones», 26 de diciembre de 2015, http://internacional.elpais.com/internacional/2015/12/26/actualidad/1451132389_125673.html).

²¹ Real Decreto 552/2014, de 27 de junio, por el que se desarrolla el Reglamento del aire y disposiciones operativas comunes para los servicios y procedimientos de navegación aérea y se modifica el Real Decreto 57/2002, de 18 de enero, por el que se aprueba el Reglamento de Circulación Aérea y Reglamento de Ejecución (UE) n.º 923/2012 de la Comisión, de 26 de septiembre de 2012, comúnmente llamado Reglamento SERA (*Standardised European Rules of the Air*).

²² Real Decreto 1919/2009, de 11 de diciembre, por el que se regula la seguridad aeronáutica de las demostraciones aéreas civiles.

el aeromodelo se capten imágenes o se recoja información de personas identificadas o identificables.

3. EL IMPACTO DEL USO CIVIL DE LOS DRONES EN LA PROTECCIÓN DE LOS DATOS DE CARÁCTER PERSONAL

En España, la norma básica aplicable al tratamiento de datos que pudiera realizarse mediante drones es la mencionada LOPD dictada en transposición de la Directiva 95/46/CE²³ que está a punto de ser sustituida por un nuevo Reglamento General de Protección de Datos al que también aludiremos en este estudio²⁴.

La LOPD no contiene ninguna disposición reguladora del uso de los drones pero su artículo 3.a define el dato personal como «cualquier información concerniente a personas físicas identificadas o identificables» en línea con la Directiva. El Reglamento de desarrollo de la LOPD (RLOPD) especifica que «cualquier información» se refiere a numérica, alfabética, fonográfica, gráfica, acústica o de cualquier otro tipo (artículo 5.1.f RLOPD)²⁵ y que es identificable «cualquier persona cuya identidad de la cual se pueda determinar, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados» (artículo 5.1 RLOPD).

Un dron puede ir equipado con una cámara fotográfica que le permita captar imágenes o llevar instalada una videocámara con la que grabar voces. Imagen y

²³ Directiva 95/46/CE sobre Protección de Datos del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

²⁴ El pasado 15 de diciembre de 2015, después de tres años de negociaciones, el Consejo, el Parlamento y la Comisión de la Unión Europea alcanzaron un acuerdo final sobre el texto del Reglamento General de Protección de Datos que tiene como objetivo la actualización de las disposiciones contenidas en la Directiva 95/46/CE. A falta de su aprobación definitiva en el Consejo y el Parlamento y de su publicación en el Diario oficial, se espera que el Reglamento entre en vigor en la primavera de 2018. El paquete legislativo de reforma del marco europeo en materia de protección de datos que propuso la Comisión en 2012 también incluye una Directiva sobre protección de datos en el ámbito policial que sustituirá a la Decisión marco 2008/977/JHA. Puede verse una versión provisional del acuerdo en <http://www.statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf>.

²⁵ Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, *BOE* núm. 17, de 19 de enero de 2008.

voz son, a los efectos de la LOPD, datos personales por lo que su su tratamiento, entendido como «las operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelar, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias» [artículo 3.c) LOPD], deberá respetar los principios y garantías establecidos en la LOPD.

Obviamente, no todos los drones cuentan con estas aplicaciones pero, como ha subrayado el Artículo 29 GT, «incluso el tipo más básico de dron equipado con componentes vitales que no procesen datos personales, puede causar molestias y perturbar a los demás. Si se le añaden otros sensores para otros fines, como grabación de datos de audio y vídeo, se plantean problemas obvios de protección de datos y privacidad»²⁶. En cualquier caso, la afectación al derecho a la protección de datos deberá analizarse en función de diversos criterios como el uso que se va a dar al dron (no plantea los mismos problemas una aeronave empleada en agricultura de precisión supervisando cultivos que aquella cuya finalidad sea la realización de tareas de vigilancia por parte de las autoridades competentes) o las tecnologías que lleve incorporadas (una simple cámara fotográfica frente a lectores de datos biométricos).

Mención aparte merece la utilización de drones en los tratamientos de datos realizados en el estricto ámbito personal.

La «excepción doméstica» está reconocida en el artículo 2.2.a LOPD que excluye de su ámbito de aplicación a «los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas». En el mismo sentido, el artículo 4.a) RLOPD añade que «sólo se consideran relacionados con actividades personales o domésticas los tratamientos relativos a las actividades que inscriben en el marco de la vida privada o familiar de los particulares». Partiendo de la premisa de que el uso habitual de drones por particulares suele enmarcarse en un contexto de ocio y de entretenimiento, por tanto, en un contexto que puede calificarse como parte de la vida privada o familiar de la persona que lo emplea, no habría ningún impedimento desde la vertiente del derecho a la protección de datos personales para utilizar este tipo de aeronaves. Así, los usuarios de drones que solo los empleen para uso personal (por ejemplo, grabarse o fotografiarse a sí mismos practicando deporte, grabaciones o fotografías en una celebración familiar, etc.) quedarán excluidos de la aplicación de la LOPD.

Fuera de este contexto, la utilización de drones por particulares con otros fines que comporte la captación y grabación de imágenes o datos de personas

²⁶ Artículo 29 GT, *Dictamen 1/2015 sobre Privacidad y Protección de Datos en relación con el uso de drones*, WP 231, 16 de junio de 2015, pág. 6, <http://ec.europa.eu/DocsRoom/documents/11481>

identificadas e identificables deberá respetar los principios y obligaciones establecidos en la LOPD. Por ejemplo, un supuesto muy común de sometimiento a esta normativa es el uso de drones por particulares para funciones de vigilancia de sus propiedades privadas cuando conlleva actividades de monitorización constante que afecten, aunque sea parcialmente, a espacios públicos²⁷.

3.1 *El tratamiento legal de la protección de datos en los usos de drones para fines públicos*

Los drones han demostrado resultar muy eficaces en tareas estatales de ciber-vigilancia realizadas por las Fuerzas y Cuerpos de Seguridad (vigilancia de fronteras, operaciones de seguimiento en alta mar, tareas de observación e investigación de sospechosos, etc.) o en programas de vigilancia masiva desarrollados por los servicios de inteligencia (vigilancia electrónica y de comunicaciones)²⁸, operaciones que deben realizarse dentro del respeto a la legalidad vigente y sometidas a las preceptivas autorizaciones judiciales, en su caso.

De lo dispuesto por el artículo 2.3.e) LOPD se deduce que el tratamiento de los datos personales procedentes de las imágenes obtenidas mediante la utilización de cámaras y videocámaras por las Fuerzas y Cuerpos de Seguridad se regirá por sus disposiciones específicas en referencia a Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos²⁹ «a fin de contribuir a asegurar la

²⁷ Véase la STJUE de 11 de diciembre de 2014, caso *František Ryněš contra Agencia de Protección de Datos Checa*, (C-212/13) en la que el Tribunal confirmó que la videovigilancia realizada por un particular sobre un área pública en el exterior de su domicilio quedaba sometida a las previsiones de la Directiva sobre Protección de Datos. La Corte señaló que la cámara también captaba imágenes de una zona pública por lo que no podía entenderse que el tratamiento de datos se había realizado en el marco de una actividad puramente personal o familiar a los efectos de la «excepción doméstica» (pár. 35).

²⁸ Sobre el tipo de controles de las comunicaciones y datos personales que realizan los servicios de inteligencia véase el valioso trabajo de SERRA CRISTÓBAL, R., «La opinión pública ante la vigilancia masiva de datos. El difícil equilibrio entre acceso a la información y seguridad nacional», *Revista de Derecho Político*, núm. 92, 2015, págs. 73 a 118.

²⁹ Debe señalarse que el Real Decreto 596/1999, de 16 de abril, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 4/1997 excluye su aplicación a las instalaciones fijas de videocámaras que realicen las Fuerzas Armadas y las Fuerzas y Cuerpos de Seguridad en sus inmuebles, siempre que éstas se dediquen exclusivamente a garantizar la seguridad y protección interior o exterior de los mismos y a las unidades de Policía Judicial cuando, en el desempeño de funciones de policía judicial en sentido estricto, realicen captaciones de imágenes y sonidos mediante videocámaras que se regirán por la Ley de Enjuiciamiento Criminal y por su normativa específica. Por tanto, en estos casos resulta de plena aplicación lo dispuesto por la LOPD y la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el

convivencia ciudadana, la erradicación de la violencia y la utilización pacífica de las vías y espacios públicos, así como de prevenir la comisión de delitos, faltas e infracciones relacionados con la seguridad pública.»

Pese a que la Ley Orgánica 4/1997 no incluye ninguna mención específica a los drones, cabe la aplicación analógica de lo dispuesto en el artículo 5 que autoriza la utilización de videocámaras móviles siempre que responda a la existencia un «peligro concreto» para la seguridad ciudadana y ajustada al principio de proporcionalidad en su doble versión de idoneidad y de intervención mínima (artículo 6 apartados 1 a 4). Además, se prevé que las imágenes y sonidos obtenidos accidentalmente, algo que sucede habitualmente con los drones, deberán ser destruidos inmediatamente por quien tenga la responsabilidad de su custodia (artículo 6.5). Este principio de proporcionalidad en el empleo de los dispositivos móviles de videovigilancia por parte de las autoridades de orden público implica que deberán evitar el rastreo cuando no sea necesario, la vigilancia indiscriminada, el tratamiento masivo de datos o la puesta en común de datos y perfiles³⁰.

La observancia de este principio de proporcionalidad ha sido destacado por la Unión Europea³¹ que subraya el hecho de que el uso de los drones por parte de las Fuerzas y Cuerpos de Seguridad y los servicios de inteligencia debe respetar el derecho fundamental a la vida privada y a la protección de datos así como las libertades de circulación y de expresión en referencia al riesgo de producir un efecto inhibitorio (*chilling effect*) del comportamiento personal³². Así, cuando las

tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras. Ambas disposiciones resultan también de aplicación a los sistemas de videovigilancia operados por el sector privado según dispone la reciente Ley 5/2014, de 4 de abril, de Seguridad Privada (artículo 42). Sobre esta cuestión, véase el Informe de la AEPD sobre Normativa aplicable a tratamientos de datos personales con fines de videovigilancia (Informe 0314/2009).

³⁰ El Artículo 29 GT recuerda que los drones deben utilizarse para finalidades explícitamente enumeradas y justificadas que deben estar fijadas de antemano y, en cualquier caso, su empleo ha de estar geográficamente acotado y limitado en el tiempo (Artículo 29 GT, *Dictamen 1/2015*, cit.).

³¹ Parlamento Europeo, *Resolución sobre el uso seguro de los sistemas de aeronaves pilotadas de forma remota (RPAS) en el ámbito de la aviación civil*, cit.

³² Nuestra jurisprudencia constitucional se ha referido al efecto disuasor o desalentador en el ejercicio de los derechos fundamentales en relación con el principio de proporcionalidad penal (véanse, entre otras, las SSTC 147/1989, de 21 de septiembre, fj 6; 37/1998, de 17 de febrero, fj 3, 136/1999, de 20 de junio, fj 21 o 110/2000, de 5 de mayo, fj 5). Según el Alto Tribunal, este efecto consiste en aquellas reacciones del poder público que, por desproporcionadas, suponen una coacción psicológica y una restricción de las libertades ciudadanas «al implicar un sacrificio desproporcionado e innecesario de los derechos fundamentales en juego que podría tener un efecto disuasorio o desalentador de su ejercicio» (STC 37/1998, de 17 de febrero, fj 3). Desde la perspectiva general de la teoría del Derecho, puede consultarse DE DOMINGO PÉREZ, T., «La argumentación

personas se encuentran sometidas a vigilancia existe una tendencia a que alteren su comportamiento y los cambios pueden ser positivos o negativos. La vigilancia abierta y consciente puede producir un efecto disuasorio (y deseable) de conductas ilegales pero cuando se tiene la sensación de estar bajo vigilancia permanente y encubierta cabe que también se produzca una modificación negativa del comportamiento. Este efecto negativo hace que las personas repriman comportamientos permitidos para ajustarse a las convenciones sociales lo que les impide ejercer sus derechos y libertades civiles legítimas como las mencionadas libertad de expresión, de circulación, de reunión o manifestación³³. La utilización de drones en funciones gubernamentales de vigilancia debe, por tanto, atenerse al cumplimiento escrupuloso del principio de idoneidad, intervención mínima y peligro concreto para no excederse en la prevalencia de la seguridad frente a los derechos individuales y provocar aquel efecto disuasor o desalentador de su ejercicio.

La autorización de cámaras móviles, supuesto que hemos asimilado a la utilización de drones, deberá aprobarse por la máxima autoridad provincial de las Fuerzas y Cuerpos de Seguridad. Esta resolución se pondrá en conocimiento de una Comisión presidida por un magistrado en la que no podrá tener mayoría la Administración solicitante en el plazo máximo de 72 horas. En cualquier caso, si la Comisión emite un informe negativo, las grabaciones deberán destruirse (artículo 5.2). El contenido de esta resolución tendría que ser equivalente, como mínimo, al previsto para las cámaras fijas (artículo 3.4) que ha de precisar el ámbito físico susceptible de ser grabado, las condiciones de uso, las especificaciones sobre el tipo de aparato y las cualificaciones del personal que lo maneja poniendo especial énfasis en la concreción de la zona sometida a videovigilancia y las limitaciones y condiciones de uso de forma que se evite la captación incidental de imágenes y datos de personas no justificadas por la finalidad del uso autorizado.

El derecho del público a ser informado sobre la existencia de videocámaras (artículo 9) también plantea una problemática específica en el caso de los drones.

jurídica en el ámbito de los derechos fundamentales: en torno al denominado «chilling effect» o «efecto desaliento», *Revista de Estudios Políticos*, núm. 122, 2003, págs. 141 a 166. En la doctrina penalista remitimos a CUERDA ARNAU, M., «Proporcionalidad penal y libertad de expresión: la función dogmática del efecto desaliento», *Revista General de Derecho Penal*, núm. 8, 2007.

³³ Sobre comportamiento personal, intimidad y efecto disuasor, véase ABRIL, P. y E. PIZARRRO MORENO, «La intimidad europea frente a la privacidad americana», *InDret*, núm. 1, 2014, págs. 8 y 9; CLARKE, R., «The regulation of civilian drones' impacts on behavioural privacy», *Computer Law and Security Review*, núm. 30, 2014, págs. 287 y 288 así como FINN, R. L., D. WRIGHT, A. DONOVAN, L. JACQUES y P. DE HERT, *Privacy, data protection and ethical risks in civil RPAS operations. D3.3: Final report for the European Commission*, 7 de noviembre de 2014, págs. 30 a 32 y la doctrina allí citada. <http://ec.europa.eu/DocsRoom/documents/8550>

Así, la previsión sobre la señalización de las zonas vigiladas se cumpliría mediante la colocación de carteles informativos («zona videovigilada por drones») cuando el dron sobrevuela un espacio público acotado pero resulta de difícil cumplimiento cuando la videovigilancia se realiza en zonas abiertas y no delimitadas como ocurre cuando se vigila una manifestación a lo largo de su recorrido por una ciudad. No habiendo medidas arbitradas, una alternativa factible para cumplir con la obligación informativa podría consistir en anuncios en medios de comunicación³⁴.

Debe destacarse que la captación, reproducción y tratamiento de imágenes y sonidos, en los términos previstos en la Ley Orgánica 4/1997, tampoco se considerarán intromisiones ilegítimas en el derecho al honor, a la intimidad personal y familiar y a la propia imagen, a los efectos de lo establecido en el artículo 2.2 de la LO 1/1982 aunque no se podrán utilizar videocámaras para tomar imágenes ni sonidos del interior de las viviendas, ni de sus vestíbulos, salvo consentimiento del titular o autorización judicial, ni de las vías públicas cuando se afecte de forma directa y grave a la intimidad de las personas, así como tampoco para grabar conversaciones de naturaleza estrictamente privada. Además, se prevé que las imágenes y sonidos obtenidos accidentalmente, algo que sucede habitualmente con los drones, deberán ser destruidas inmediatamente, por quien tenga la responsabilidad de su custodia (artículo 6.5). El plazo de cancelación del resto de grabaciones es de un mes desde su captación salvo las que contengan imágenes relacionadas con infracciones penales o administrativas graves, con la correspondiente obligación de reserva por parte de los que tengan acceso a las imágenes (artículo 8).

Por último, resta señalar que al tratamiento de imágenes y sonidos se les aplica supletoriamente la LOPD en aspectos concretos, por ejemplo, a las videocámaras con fines de control de tráfico (Disposición Adicional Octava de la Ley Orgánica 4/1997). De hecho, el empleo de drones con esta finalidad y otras relacionadas con la monitorización y gestión del tráfico en las carreteras está proyectado en algunos países como Francia y España³⁵. En nuestro caso, su uso requerirá la modificación de la actual legislación que, como vimos, obliga a mantener la aeronave dentro del alcance visual del piloto con lo que no es posible que monitorice a cientos de kilómetros.

³⁴ ELODI VILLENA, M., «El uso de vehículos aéreos no tripulados (drones) en las labores de seguridad y vigilancia de la Administración», en *Congreso Derecho TICS - SICARM 2014*, Barcelona, 23-24 de octubre de 2014, pág. 6.

³⁵ REDONDO, M., «DGT quiere probar drones que controlen el tráfico en 2016», 22 de octubre de 2015, <http://www.autobild.es/noticias/dgt-desarrolla-dron-que-controla-trafico-269967>.

3.2 *El cumplimiento de los principios de la LOPD por el operador de un dron para fines privados*

Centrándonos en el uso profesional o comercial de los drones y a la vista de las actividades autorizadas por la regulación actual es posible que se den supuestos en los que no se produce un tratamiento de datos personales a los efectos de la LOPD y que, por tanto, esta normativa no resulte de aplicación (por ejemplo, para la captación de imágenes paisajísticas, de edificios arquitectónicos o panorámicas para fines turísticos, promocionales, de publicidad o de documentación patrimonial, entre muchas otras). Sin embargo, dadas la flexibilidad de movimientos y el tipo de emplazamientos en los que habitualmente se emplean estas aeronaves, es factible que en algún momento se puedan captar imágenes de personas físicas identificadas o identificables lo que obligará a tener presentes los principios y obligaciones de la LOPD.

La regla básica del régimen jurídico de la protección de datos personales en nuestro país es la del consentimiento inequívoco de los afectados o la autorización legal explícita para que terceros puedan disponer lícitamente de datos personales. Junto con el consentimiento, los principios configuradores del derecho a la protección de datos son los recogidos en el artículo 4 LOPD, principios relativos a la calidad de los datos para cuya efectividad se requiere el reconocimiento de los derechos regulados en los artículos 15 y 16 LOPD, esto es, los derechos de acceso, rectificación, cancelación y oposición (derechos ARCO) del titular de los datos.

Atendiendo a estos elementos clave, podemos identificar los siguientes riesgos en relación con el tratamiento de datos personales que pueden llevar a cabo los drones cuando se emplean para fines particulares o comerciales.

En primer lugar, el *principio de información* que exige que los interesados sean previamente informados de modo expreso, preciso e inequívoco de la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de su recogida y de los destinatarios de los mismos (artículo 5 LOPD). Asimismo, debe notificarse a la Agencia Española de Protección de Datos la creación de un registro figurando necesariamente la identificación del responsable del fichero, su finalidad, el tipo de datos que contiene y las medidas de seguridad para su protección (artículo 26 LOPD).

El cumplimiento de este principio obliga a que la información que se suministre a los titulares de los datos incluya la identidad del operador del dron o su representante, los fines a los que se destinan los datos recogidos, la categoría de datos sometidos a tratamiento, los destinatarios de esos datos así como los derechos que asisten a los sujetos titulares. Esta información debería facilitarse en el

momento en el que se solicita el consentimiento inequívoco del afectado tal y como exige el artículo 6 LOPD que no contempla los fines comerciales o profesionales entre los supuestos excepcionados de este requisito³⁶. Además, el consentimiento habrá de ser expreso y por escrito si los drones se emplean en espacios que, por su naturaleza o características, pueden comportar la captación de imágenes que pudieran revelar la ideología, afiliación sindical, la religión o las creencias de las personas afectadas (artículo 7 LOPD). Entre las excepciones a la obligación de solicitar el consentimiento destaca la previsión del artículo 8.2.c) de la LO 1/1982 que habilita la captación y el tratamiento de imágenes de personas físicas identificadas o identificables mediante drones, tanto en espacios públicos como en espacios cerrados en los que tenga lugar un evento público, siempre que dichas imágenes aparezcan como meramente accesorias.

La cuestión que se plantea es, básicamente, de qué modo cabe dar cumplimiento a la cláusula informativa cuando se produce un tratamiento de datos mediante el uso de drones.

En el caso de utilización de drones en recintos cerrados, la información podría facilitarse en el momento en que se solicita el consentimiento de los afectados o mediante la instalación de carteles informativos³⁷. Estos carteles también servirían para cumplir con la obligación informativa en el caso de uso de drones en recintos abiertos delimitados. Mayor complejidad presentan los espacios abiertos no delimitados por lo que es necesario arbitrar propuestas alternativas para lograr

³⁶ Artículo 6.2 LOPD: «No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación comercial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado».

³⁷ La Agencia Catalana de Protección de Datos especifica que: primero, se deberían colocar tantos carteles como fueran necesarios para garantizar que las personas afectadas tienen conocimiento del uso de drones en el espacio cerrado al que pretenden acceder y ubicarlos en emplazamientos claramente visibles en cada uno de los accesos del espacio cerrado de que se trate; segundo, deberán colocarse los carteles antes de que se empleen los drones y sólo podrían retirarse una vez finalizara su uso; tercero, el contenido de estos carteles debería, como mínimo, permitir conocer a las personas afectadas que en el espacio al que quieren acceder están utilizando drones y que, por tanto, su imagen podría ser captada por estas aeronaves, la finalidad de su uso y la identificación de la persona responsable ante la que se pueden ejercer los derechos ARCO (Agencia Catalana de Protección de Datos, *Informe 12/2014 en relación con la consulta planteada por una universidad sobre el ejercicio los derechos ARCO en el uso de «drones»*, de 17 de marzo de 2014).

un nivel razonable de información a los ciudadanos. Esto podría lograrse a través de la publicidad insertada en el sitio web de la organización con la información básica sobre el anuncio del vuelo (área, itinerario, duración) y la relacionada con aspectos como periodos de conservación de las imágenes y otros datos personales, modos de ejercicio de los derechos de acceso, cancelación y oposición o identificación sobre la persona o empresa responsable del tratamiento³⁸. También se ha sugerido que, a la vista de las circunstancias concretas concurrentes en cada caso, el responsable se dirigiera ante la Agencia de Protección de Datos para exponer «qué medios tiene pensado emplear para dar cumplimiento al deber de información a los afectados para que la Autoridad pudiera pronunciarse sobre su adecuación a la normativa de protección de datos y, en su caso, proponer (medios) complementarios o sustitutivos»³⁹.

Porque, efectivamente, si los ciudadanos no son conscientes de la presencia de drones que realizan un tratamiento de datos personales no podrán ejercer adecuadamente sus derechos lo que conecta directamente con el *principio de responsabilidad* y el cumplimiento de los deberes que corresponde al operador del dron. Aún en el caso de percatarse, difícilmente ejercerán los derechos ARCO si no poseen información – datos de contacto – del operador del mismo o de las finalidades de la recogida. Como establece la STC 292/2000 «(...) son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele» (fj 7).

Entendemos que también puede resultar especialmente útil a estos efectos la realización de evaluaciones de impacto en relación con la protección de datos personales que han sido sugeridas desde algunas autoridades de protección de datos europeas, destacadamente, la AEPD que contiene esta sugerencia en su *Guía*

³⁸ GUERRERO LEBRÓN, M. J., C. CUERNO REJADO y P. MÁRQUEZ LOBILLO, «Aeronaves no tripuladas. Estado de la legislación para realizar su integración en el espacio aéreo no segregado», *op. cit.*, pág. 102.

³⁹ Agencia Catalana de Protección de Datos, *Informe 12/2014 en relación con la consulta planteada por una universidad sobre el ejercicio los derechos ARCO en el uso de «drones»*, cit.

para una evaluación de impacto en la protección de datos personales⁴⁰. Sugerencia que pasará a convertirse en exigencia legal cuando entre en vigor la Propuesta de Reglamento General de Protección de Datos, que obliga al responsable del tratamiento a la realización de evaluaciones de impacto «cuando las operaciones entrañen riesgos específicos para los derechos y libertades de los interesados en razón de su naturaleza, alcance o fines» (artículo 33 de la Propuesta). En este tipo de operaciones se engloban algunas que encajan en las posibles actividades realizadas mediante un dron, a saber, la evaluación sistemática y exhaustiva de los aspectos personales propios de una persona física o destinada a analizar o a predecir, en particular, localización, preferencias personales o comportamiento, que se base en un tratamiento automatizado y sobre la base de la cual se tomen medidas que produzcan efectos jurídicos que atañan o afecten significativamente a dicha persona; el seguimiento de zonas de acceso público, en particular cuando se utilicen dispositivos optoelectrónicos (videovigilancia) a gran escala y el tratamiento de datos personales en ficheros a gran escala relativos a niños, o el tratamiento de datos genéticos o biométricos [artículo 33.2 apartados a), c) y d) de la Propuesta]. La ventaja de la evaluación de impacto es que introduce una actuación preventiva que minimiza los posibles efectos negativos que el uso de los drones puede provocar en la esfera de la vida privada y la protección de datos de los ciudadanos, por ejemplo, mediante una completa y clara descripción de los límites geográficos y la duración en los que se desenvuelven las operaciones de drones⁴¹.

El principio de calidad de los datos también se pone en riesgo, en segundo lugar, cuando no se observa la *finalidad del tratamiento* que implica que los datos de carácter personal objeto de tratamiento no puedan usarse para finalidades incompatibles con aquellas para las que hubieran sido recogidos (artículo 4.2 LOPD). Esta exigencia debe analizarse en relación con la exigencia de *proporcionalidad de los datos*. Según el artículo 4.1 LOPD los datos de carácter personal sólo se podrán recoger para su tratamiento cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades, explícitas y legítimas para las que se hayan obtenido.

⁴⁰ AEPD, *Guía para una evaluación de impacto en la protección de datos personales*, 29 de octubre de 2014, https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf. Véase también el *Código de Prácticas para la Evaluación de Impacto en la Protección de Datos* de la Oficina del Comisionado de Información en Reino Unido (febrero de 2014, <https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf>) y la *Guía sobre el uso de drones* publicada por el Comisionado para la Protección de Datos en Irlanda (22 de diciembre de 2015, <https://www.dataprotection.ie/docs/Guidance-on-the-use-of-Drone-Aircraft/1510.htm>).

⁴¹ ACED FÉLEZ, E., «Drones: una nueva era de la vigilancia y de la privacidad», *Seguritecnia*, núm. 403, 2013, pág. 64.

La grabación y el tratamiento de datos mediante el uso de drones plantea riesgos añadidos en relación con los principios de finalidad y proporcionalidad porque, a diferencia de otros sistemas de vigilancia como las CCTV, los drones son aéreos, móviles, discretos y pueden ir equipados con sofisticadas tecnologías que permiten el almacenamiento masivo e indiscriminado de datos. O incluso procediéndose a una recogida selectiva de datos para una finalidad determinada, pueden utilizarse esos datos para fines distintos. Sería el caso del empleo de drones para realizar tareas de seguridad en una empresa pero, a la vez, aprovechar la información recabada para vigilar a los trabajadores. Es la técnica que se ha bautizado como «desviación de uso» (*function creep*).

Un tercer aspecto problemático es el relacionado con la *seguridad*. El artículo 4.5 LOPD protege la integridad de los datos y obliga a su cancelación cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. Por su parte, el artículo 9 LOPD concreta este principio que implica, básicamente, que es necesario adoptar las medidas de índole técnica y organizativas que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado.

En el caso de los drones, la transmisión de los datos capturados se hace a través de comunicaciones inalámbricas que no es una tecnología que ofrezca garantías fiables de seguridad y puede poner en riesgo la integridad y la confidencialidad de los datos personales. Por ello, los datos almacenados y sometidos a tratamiento por drones tendrán que ser eliminados o anonimizados bien porque han sido capturados de manera incidental o accidental cuando no eran el objetivo de la utilización del dron bien porque ha expirado el plazo para alcanzar su finalidad. Su mantenimiento durante un periodo más prolongado puede suponer un elevado riesgo de pérdida o robo para ser utilizados para dañar la intimidad de los titulares de los datos o, incluso, para cometer posteriormente otros actos delictivos. Como concreta el Artículo 29 GT «por ejemplo, las imágenes o vídeos grabados por drones para realizar tareas de seguridad durante un concierto al aire libre solo deberán ser conservados durante el tiempo necesario para investigar posibles quejas o cuestiones relacionadas con la seguridad»⁴².

Por último, debemos referirnos a la *prohibición de elaboración de perfiles*. La técnica del *profiling* consiste en un proceso de acumulación y análisis masivo de datos de carácter personal para la elaboración de bases de datos que se puedan utilizar para realizar valoraciones o tomar decisiones sobre los sujetos⁴³. El artí-

⁴² Artículo 29 GT, *Dictamen 1/2015*, cit., pág. 17.

⁴³ Un ejemplo de esta técnica lo constituye la instalación de cookies que rastrean nuestra actividad online para ofrecer publicidad de productos y servicios adaptada a nuestros gustos o

culo 36 RLOPD⁴⁴ establece que los interesados tienen derecho a no verse sometidos a una decisión con efectos jurídicos sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, tales como su rendimiento laboral, crédito, fiabilidad o conducta.

La elaboración de perfiles se considera una operación de riesgo⁴⁵ porque si bien por un lado, ha sido utilizada provechosamente por el sector público para predecir patrones de comportamiento de riesgo en la población y tomar decisiones para atajar actividades delictivas o en la lucha antiterrorista, por otro lado, esta técnica puede provocar discriminación mediante la identificación de las personas o grupos sociales para aplicarles un tratamiento desfavorable basado en suposiciones erróneas. Estos riesgos caben darse en los tratamientos de datos realizados por algún tipo de drones equipado con tecnologías de reconocimiento facial y biométrico que hace posible monitorizar a individuos en función de parámetros como el sexo, edad o raza. Asimismo, los drones también pueden llevar instaladas cámaras específicas que están programadas para detectar comportamientos anormales o peligrosos mediante la utilización de programas de algoritmos inteligentes que discriminan a las personas basándose igualmente en criterios biométricos.

4. PROPUESTAS PARA UN MARCO REGULADOR ARMONIZADO EN RELACIÓN CON LA PROTECCIÓN DE DATOS Y LAS OPERACIONES DE DRONES CIVILES

El panorama descrito ha provocado una intensa labor institucional para analizar los retos que los drones plantean a la intimidad y la protección de datos y enunciar numerosas propuestas de solución de diversa naturaleza.

Estas recientes iniciativas proceden básicamente del entorno europeo y han tomado como punto de partida la Comunicación de la Comisión Europea adopta-

hábitos. Sobre la cuestión, véase AEPD, *Guía sobre el uso de las cookies*, 29 de abril de 2013, http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_Cookies.pdf así como Artículo 29 GT, *Dictamen 4/2012 sobre la exención del requisito de consentimiento de cookies*, WP 194, 7 de junio de 2012, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_es.pdf

⁴⁴ Véase también el artículo 15 de la Directiva 95/46/CE y el artículo 20 de la Propuesta de Reglamento.

⁴⁵ Artículo 29 GT, *Documento de asesoramiento sobre los elementos esenciales para una definición y regulación de la técnica de elaboración de perfiles en la Propuesta de Reglamento de Protección de Datos*, 13 de mayo de 2013. http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130513_advice-paper-on-profiling_en.pdf

da en abril de 2014 sobre *Una nueva era para la aviación: Abriendo el mercado aéreo al uso civil de los drones de forma segura y sostenible* que marca el punto de inflexión a partir del cual las problemáticas relacionadas con la privacidad y la protección de datos son objeto de estudio específico y de declaraciones institucionales clave en Europa⁴⁶. Concretamente, la Comunicación dispone que las operaciones realizadas por drones «no deberán ser de naturaleza tal que infrinjan los derechos fundamentales, incluidos el derecho a la intimidad personal y familiar y la protección de los datos personales. Dentro de la amplia gama de aplicaciones civiles potenciales de los drones, los hay que pueden implicar la recogida de datos personales y suscitar problemas de orden ético, de protección de la intimidad o de datos personales, en particular en los ámbitos de la vigilancia, el seguimiento, la cartografía o los registros de vídeo. Los operadores de drones tendrán que cumplir las disposiciones aplicables en materia de protección de datos, en particular las indicadas en las medidas nacionales establecidas de conformidad con la Directiva 95/46/CE sobre la protección de los datos personales y la Decisión Marco 2008/977»⁴⁷.

En respuesta a la Comunicación se han adoptado varios dictámenes que proponen mecanismos nuevos y herramientas concretas para garantizar la conformidad de las aplicaciones de los drones con las normas de protección de datos. Se trata, en primer lugar, del *Dictamen sobre Ética de las Tecnologías de la Seguridad y la Vigilancia* emitido en mayo de 2014 por el Grupo Europeo en Ética de las Ciencias y las Nuevas Tecnologías enfocado a evaluar el uso de los drones en misiones de vigilancia. Seguidamente, en noviembre de ese mismo año, el Supervisor Europeo de Protección de Datos publicó su *Dictamen sobre la Comunicación de la Comisión Europea «Una nueva era para la aviación»*⁴⁸ y un grupo de expertos elaboró para la Comisión Europea el *Estudio sobre privacidad, protección de datos y riesgos éticos en las aeronaves civiles pilotadas por control remoto* elaborado para la Comisión Europea por un grupo de expertos en noviembre 2014⁴⁹. Por último,

⁴⁶ Destaca, en especial, la *Declaración de Riga* adoptada por la comunidad aeronáutica que respaldó unánimemente los objetivos especificados en la Comunicación de la Comisión (Declaración de Riga sobre Aeronaves Pilotadas por Control Remoto (drones), *Un marco para el futuro de la aviación*, 6 de marzo de 2015. https://eu2015.lv/images/news/2016_03_06_RPAS_Riga_Declaration.pdf).

⁴⁷ Comisión Europea, *Una nueva era de la aviación. Abrir el mercado de la aviación al uso civil de sistemas de aeronaves pilotadas de forma remota de manera segura y sostenible*, cit., págs. 8 y 9.

⁴⁸ Grupo Europeo en Ética de las Ciencias y las Nuevas Tecnologías, *Dictamen sobre Ética de las Tecnologías de la Seguridad y la Vigilancia* (n.º 28), 20 de mayo de 2014, <http://ec.europa.eu/DocsRoom/documents/11493>

⁴⁹ Supervisor Europeo de Protección de Datos, *Dictamen sobre la Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre «Una nueva era para la aviación. Abrir el mercado de la aviación al uso civil de sistemas de aeronaves pilotadas de forma remota de manera segura y sostenible»*, 26 de noviem-

las Autoridades Europeas de Protección de Datos (Artículo 29 GT) adoptaron en junio de 2015 su *Dictamen sobre Privacidad y Protección de Datos en relación con el uso de drones*⁵⁰ que ha servido de base para redactar la mencionada *Resolución sobre el uso seguro de los sistemas de aeronaves pilotadas de forma remota (RPAS) en el ámbito de la aviación civil* que fue aprobada por el Parlamento Europeo en su sesión plenaria del 29 de octubre de 2015.

En estos documentos se subraya que los derechos a la vida privada y familiar y a la protección de datos, tal como quedan garantizados en el artículo 8 del Convenio Europeo de Derechos Humanos y en los artículos 7 y 8 de la Carta de Derechos Fundamentales de la Unión Europea, resultan aplicables a esta tecnología emergente y se advierte que ambos derechos son elementos fundamentales a la hora de favorecer el desarrollo y la incorporación segura de los drones en la aviación civil. Además, se analiza en profundidad la normativa aplicable en materia de protección de datos en todos los Estados miembros en el momento de su aprobación, esto es, la Directiva 95/46/CE complementada con lo dispuesto en la Directiva 2002/58 de Privacidad y Comunicaciones Electrónicas⁵¹.

Las recomendaciones y propuestas de solución contenidas en estos trabajos son de diversa naturaleza y pueden clasificarse en sugerencias de carácter normativo o legal, soluciones técnicas y reglas voluntarias o de autorregulación.

Por lo que se refiere a la *adopción de medidas legislativas*, a nivel europeo se confía en que la aprobación e implementación de la Propuesta de Reglamento servirá para hacer frente a los retos que el uso civil y comercial de los drones plantean para los derechos a la protección de datos y a la vida privada de los ciudadanos. Ya nos hemos referido al positivo papel que, en este sentido, jugarían las evaluaciones de impacto a lo que cabría añadir la previsión de la figura del Delegado de Protección de Datos (artículo 35 de la Propuesta de Reglamento) que se encargaría de supervisar el uso adecuado de los datos personales obtenidos por los drones, proporcionar directrices para diseñar los tratamientos de datos, garantizar la adopción de las medidas de seguridad necesarias y actuar como medio de enlace con el público.

Por otra parte, se sugiere la revisión de algunas normas de aplicación a los usos civiles de los drones como es el caso de la mencionada Directiva sobre Privacidad y Comunicaciones Electrónicas para extender su aplicación a nuevas

bre de 2014. https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-11-26_Opinion_RPAS_EN.pdf

⁵⁰ Artículo 29 GT, *Dictamen 1/2015*, cit.

⁵¹ Directiva 2002/58 del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. <http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32002L0058>

tecnologías como la Voz sobre protocolo de Internet (VoIP) que son los recursos que hacen posible que la señal de voz se transmita a través de Internet en forma digital o en paquetes de datos o la incorporación de las redes privadas empresariales en el campo de aplicación de la Directiva⁵².

Finalmente, se ha señalado la oportunidad de aprobar una ley específica que se ocupe de la regulación del uso civil de los drones⁵³, tarea en la que está inmersa la Unión Europea y que debería culminarse cuanto antes. En este sentido, se señala que los siguientes extremos deberían ser incorporados en el contenido de la disposición: las obligaciones y condiciones que recaen sobre los operadores de drones para uso civil (con estrictas limitaciones sobre el tipo de tecnologías a instalar en las aeronaves), las categorías de datos que un dron está autorizado a recopilar o el plazo máximo de almacenamiento de datos, entre otros.

Las *soluciones basadas en la tecnología* parten de la idea que la tecnología es una herramienta neutra para resolver los problemas que plantea el tratamiento de datos en la era de la comunicación global. Los datos y la información son procesados por individuos situados en cualquier parte del mundo y sometidos a distintas jurisdicciones. Así, ante la ausencia de reglas comunes en materia de privacidad y protección de datos, la tecnología se presenta como un instrumento neutral y objetivo. La privacidad por diseño, la privacidad por defecto o las evaluaciones de impacto de la protección de datos son conocidos ejemplos de las denominadas Tecnologías de Protección de la Intimidad (PET)⁵⁴ que garantizan no sólo que cualquier violación de las normas de protección de datos es una actividad prohibida y sujeta a sanción, sino también técnicamente más difícil de llevar a cabo. No menos importante es la ventaja de que tomar medidas preven-

⁵² Grupo Europeo en Ética de las Ciencias y las Nuevas Tecnologías, *Dictamen sobre Ética de las Tecnologías de la Seguridad y la Vigilancia*, cit., pág. 90.

⁵³ Artículo 29 GT, *Dictamen 1/2015*, cit., pág. 19. También VOLOVELSKY, U., «Civilian uses of unmanned aerial vehicles and the threat to the right to privacy. An Israeli case study», *Computer Law & Security Review*, núm. 30, 2014, pág. 319.

⁵⁴ Comisión Europea, *Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el fomento de la protección de datos mediante las tecnologías de protección del derecho a la intimidad (PET)*, COM(2007)228 final, Bruselas, 14 de mayo de 2007. <http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=URISERV:l14555&from=EN>. La privacidad por diseño implica que la protección de la privacidad está integrada en el sistema desde el momento inicial de su diseño; la privacidad por defecto significa que el sistema se configura de modo que, por defecto, otorga una mayor protección a la privacidad de las personas, por ejemplo, impidiendo que se comparta la información del usuario salvo que este modifique la conformación del sistema y la evaluación de impacto de protección de datos es un ejercicio de análisis de riesgos en el que se identifican las posibles amenazas para la privacidad que implica el proceso o sistema que se evalúa.

tivas resulta más eficaz y justo que cualquier otra medida reactiva como sanciones económicas por violaciones de las normas sobre protección de datos.

En esta línea, el Grupo Europeo en Ética de las Ciencias y las Nuevas Tecnologías explica que tanto las empresas privadas como las autoridades públicas en Europa deben adoptar los principios de las PET en el desarrollo de las nuevas tecnologías de vigilancia y seguridad porque «los valores europeos de dignidad, libertad y justicia deben tenerse en cuenta antes, durante y después del proceso de diseño, desarrollo y ejecución de esas tecnologías. Las tecnologías de protección de la intimidad deben incorporarse desde la fase inicial y no añadirse como un apéndice posteriormente»⁵⁵.

Por su parte, el Dictamen del Supervisor Europeo recuerda que estas herramientas estarán claramente recogidas en la Propuesta de Reglamento (artículos 23 y 33, respectivamente)⁵⁶ y apunta algunos ejemplos de privacidad por diseño como, en primer lugar, la incorporación de programas de almacenamiento y borrado de datos de forma que las aplicaciones y tecnologías incorporadas en los drones se proyecten de tal modo que garanticen el almacenamiento seguro de datos durante un periodo de tiempo superado el cual serían eliminados automáticamente. En segundo término, el diseño de los drones también debería flexibilizarse para permitir que cada comprador pudiera seleccionar con qué tipo de dispositivos desea equipar la aeronave en función de la finalidad de su negocio. Esta flexibilidad les facultaría para elegir la tecnología menos invasiva para la privacidad o la protección de datos, por ejemplo, un dron empleado para trazar mapas de carreteras no necesitará una cámara de alta resolución que le permita identificar las matrículas de los vehículos. Por último, las interferencias en la vida privada o en la protección de datos podrían evitarse mediante funcionalidades respetuosas con los datos personales (*data protection friendly functionalities*) como la posibilidad de incorporar sensores de encendido y apagado durante el

⁵⁵ Grupo Europeo de Ética de las Ciencias y las Nuevas Tecnologías, *Dictamen sobre Ética de las Tecnologías de la Seguridad y la Vigilancia*, cit., pág. 91.

⁵⁶ Supervisor Europeo de Protección de Datos, *Dictamen sobre la Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre «Una nueva era para la aviación»*, cit., pág. 10. Véase también el Dictamen 58/2013 de la Agencia Catalana de Protección de Datos en el que aconseja la adopción del empleo de programas de análisis de vídeo para evitar la captación de imágenes de personas físicas o bien su identificación (Agencia Catalana de Protección de Datos, *Dictamen en relación con la consulta planteada por una universidad pública sobre cuál es el marco legal para el uso tanto particular como comercial de los «drones»*, de 18 de diciembre de 2013), mecanismo considerado válido por la AEPD en su investigación sobre Google Street View (AEPD, *Resolución sobre campaña de recogida de datos para el servicio Google Street View*, 14 de marzo de 2013).

vuelo, ocultación automática de áreas privadas o desdibujado de rostros cuando las imágenes han sido grabadas fortuitamente⁵⁷.

Finalmente, existe un grupo de propuestas enfocadas desde una *perspectiva social o voluntaria*. Todas estas soluciones se fundamentan en la creencia de que la información, la educación y la asunción de responsabilidades son elementos clave para establecer un clima de confianza y aceptación generalizada de los drones.

El uso doméstico de estas aeronaves es una seria preocupación para autoridades, legisladores y público en general puesto que muchas violaciones de la protección de datos y la vida privada y familiar pueden ser el resultado de un empleo inadecuado o poco ético de los drones por particulares. Como hemos señalado antes, mientras que el uso profesional y comercial de los drones está completamente sometido a las normas de protección de datos, otros usos – doméstico, recreativo o deportivo – pueden no estarlo. Por ello, se propone que el uso doméstico sea sometido a una autorización previa y un adecuado seguimiento o control que garantice la seguridad del vuelo y evite abusos⁵⁸. Concretamente, endureciendo los requisitos para aquellos particulares que deseen utilizar un dron con fines de vigilancia quienes deben demostrar que el uso propuesto es legítimo, necesario y proporcionado. O facilitando que las normas y procedimientos aplicables al uso doméstico de drones para fines de vigilancia sean de acceso público en aras de una mayor transparencia.

Otra iniciativa es la creación de un sistema de registro *online*⁵⁹. Esta base de datos se utilizaría por los pilotos de drones comerciales para informar acerca de sus planes de vuelo, política de protección de datos lo que aumentaría la transparencia y permitiría a los ciudadanos identificar el operador así como otra información útil para el ejercicio de sus derechos. En la misma línea de facilitar el máximo de información se sugiere la elaboración de mapas en los que queden

⁵⁷ Supervisor Europeo de Protección de Datos, *ibid.*, pág. 15. El Parlamento Europeo se suma a estas consideraciones y, entre las soluciones para el futuro, pide a la Comisión que vele por que, en el desarrollo de cualquier política de la Unión Europea sobre drones de uso comercial, se incorporen garantías relativas a la protección de la vida privada y de los datos incluyendo entre los requisitos mínimos la obligación de realizar evaluaciones de impacto y de proteger la vida privada, desde el diseño y por defecto (Parlamento Europeo, *Resolución sobre el uso seguro de los sistemas de aeronaves pilotadas de forma remota (RPAS) en el ámbito de la aviación civil*, cit., apartados 24 y 25).

⁵⁸ Grupo Europeo de Ética de las Ciencias y las Nuevas Tecnologías, *Dictamen sobre Ética de las Tecnologías de la Seguridad y la Vigilancia*, cit., pág. 89.

⁵⁹ House of Lords, European Union Committee, *Civilian use of drones in UE*, 5 March 2015, págs. 41, 48 y 69. <http://www.publications.parliament.uk/pa/ld201415/ldselect/lddeu-com/122/122.pdf>

claramente delimitadas las zonas donde el vuelo de drones está permitido⁶⁰. En cuanto a los operadores de estos aparatos, el Artículo 29 GT aconseja evitar en lo posible volar sobre zonas privadas y edificios, incluso cuando esté permitido su uso.

También se ha manifestado preocupación en torno al desconocimiento entre los operadores de drones en relación con sus responsabilidades en materia de protección de datos y privacidad. Por ello se sugiere la publicación de guías para operadores de drones sobre el impacto de esa legislación en su actividad⁶¹. Este es el caso de algunos países cuyas Agencias de Protección de Datos están desarrollando una actividad muy intensa en la difusión de información sobre drones: en Reino Unido, la ICO ha revisado el Código de Prácticas sobre CCTV para incorporar la tecnología de los drones⁶², la Comisión Nacional de la Informática y las Libertades en Francia ha publicado varios artículos enfocados al uso de drones y la videovigilancia⁶³, la Comisión para la Protección de la Privacidad belga ha incorporado recientemente una página sobre preguntas frecuentes relativas a la utilización de drones⁶⁴ o el caso ya mencionado de Guía para uso de drones editado por el Comisionado irlandés para la Protección de Datos. Para complementar esta tarea, se apuesta por la promoción de códigos de conducta o autorregulación elaborados por los fabricantes o los operadores de estas aeronaves lo que contribuirá a sensibilizar y a responsabilizar a estos colectivos en materia de protección de datos⁶⁵.

Finalmente, desde el Parlamento Europeo se fomenta la educación como la mejor arma para instruir acerca de los beneficios e informar sobre los perjuicios derivados del uso de los drones y se invita a los Estados miembros a que se ase-

⁶⁰ Artículo 29 GT, *Dictamen 1/2015*, cit., pág. 19.

⁶¹ House of Lords, *Civilian use of drones in UE*, cit., pág. 65.

⁶² Information Commissioner's Office, *In the picture: A data protection code of practice for surveillance cameras and personal information*, Version 1.1, 21 de mayo de 2015.

⁶³ Destacamos las siguientes publicaciones: Commission nationale de l'informatique et des libertés, *Usages des drones et protection des données personnelles*, 30 de octubre de 2012, <http://www.cnil.fr/institution/actualite/article/article/usages-des-drones-et-protection-des-donnees-personnelles>, *Drones: quelle vision prospective, quels enjeux pour les libertés?*, 6 de diciembre de 2013, <http://www.cnil.fr/institution/actualite/article/article/drones-quelle-vision-prospective-quels-enjeux-pour-les-libertes/>

⁶⁴ Commission for the Protection of Privacy, *Privacy Commission responds about drones. FAQ section*, <http://www.privacycommission.be/en/node/16643>

⁶⁵ Sobre el fomento de las iniciativas de autorregulación, véase AEPD, *Contribución de la Agencia Española de Protección de Datos a la Consulta de la Comisión sobre un enfoque global de la protección de datos personales en el marco de la Unión Europea*, 3 de marzo de 2011. http://ec.europa.eu/justice/news/consulting_public/0006/contributions/public_authorities/aepd_dpa_es.pdf

guren de que, en el marco de la formación ofrecida a usuarios profesionales y propietarios de drones, se incluya formación específica sobre protección de datos y de la vida privada⁶⁶. La ciudadanía debe conocer las implicaciones que tiene el empleo de las tecnologías de seguridad y vigilancia (cómo, por qué y para qué finalidad se recogen y tratan los datos personales) y los operadores de drones civiles tienen que ser conscientes de las consecuencias y las responsabilidades derivadas de sus actividades sobre los derechos a la protección de datos y la privacidad.

5. REFLEXIONES FINALES

La proliferación del uso civil de los drones en todo el mundo es una realidad que confirmamos a diario con noticias sobre las nuevas aplicaciones y los futuros usos que se pretenden dar a esta tecnología emergente. Su versatilidad funcional y su bajo coste los han convertido en un producto de consumo masivo y tanto la Unión Europea como los Estados miembros están desarrollando normativa que permita aprovechar los numerosos beneficios y el potencial económico y social de estas aeronaves pilotadas por control remoto.

Sin embargo, el desarrollo de este mercado encuentra obstáculos originados, básicamente, por dos cuestiones. En primer lugar, un todavía limitado reconocimiento de las actividades que pueden realizarse con ellos unido a un rígido marco legal que impone unas condiciones muy estrictas para aquellas actividades que sí están permitidas. Esta situación está provocada por la inexistencia de una regulación armonizada que garantice la seguridad de los vuelos de drones civiles. La explotación de esta nueva tecnología pasa necesariamente por la aprobación de soluciones técnicas y normativas que permitan la integración de este tipo de aeronaves con la aviación convencional en el espacio aéreo así como por la necesidad de desarrollar un proceso de reconocimiento mutuo de las certificaciones y autorizaciones expedidas por los diferentes países dentro del entorno europeo, objetivos harto complicados debido tanto a la extensión de las áreas a las que afecta como a la necesidad de alcanzar soluciones globalmente aceptadas. En segundo término, una aplicación insuficiente de la normativa en materia de protección de datos. Ante el crecimiento imparable del número de drones utilizado con fines profesionales y comerciales pero, sobre todo, para usos recreativos y deportivos, aumenta la conciencia de los ciudadanos ante posibles violaciones

⁶⁶ Parlamento Europeo, *Resolución sobre el uso seguro de los sistemas de aeronaves pilotadas de forma remota (RPAS) en el ámbito de la aviación civil*, cit., apartado 31.

de su intimidad y protección de datos y también es mayor la presión social para que se controlen estos abusos.

A falta de desarrollo de un marco legal específico, entendemos que la aplicación rigurosa de la actual normativa en materia de protección de datos permitiría garantizar estos derechos puesto que los problemas que los drones plantean en relación con la protección de datos no son nuevos ya que las tecnologías que utilizan tampoco lo son. La novedad se deriva de las características de estos aparatos —su movilidad, su reducido tamaño, su invisibilidad, la compleja tecnología con la que pueden ir equipados— que los convierten en sistemas de vigilancia que pueden tener un efecto inhibitorio en el comportamiento de los ciudadanos que les impida el ejercicio de derechos y libertades civiles legítimas.

En este sentido, tanto la Directiva 95/46/CE —en breve, el Reglamento General de Protección de Datos— como la LOPD determinan con claridad los principios básicos sobre los que se asienta la regulación del derecho a la protección de datos y, a pesar de que no contienen ninguna mención específica al uso civil de drones, les resultan de aplicación. Así ocurre con la obligación de informar al usuario sobre la recogida y tratamiento de sus datos, el principio del consentimiento y el de calidad de los datos, los derechos de los titulares de los datos —acceso, rectificación, cancelación y oposición—, la necesidad y proporcionalidad en la captura y el tratamiento de los datos, las obligaciones de los responsables del tratamiento, etc.

Es cierto que la aplicación de este marco general ha revelado insuficiencias para afrontar algunos riesgos concretos que hemos ido señalando a lo largo de nuestro estudio, destacadamente, las dificultades para cumplir con la obligación informativa cuando el vuelo del dron se opera en espacios abiertos y no delimitados lo que repercute en la prestación del consentimiento y el ejercicio de los derechos ARCO o los problemas particulares que la recopilación masiva de datos por drones plantea frente al principio de proporcionalidad. Se trata de situaciones para las que se han aportado numerosas sugerencias desde diversas perspectivas —medidas de tipo legislativo, tecnológico o de autorregulación—, la mayor parte de las cuales se ensayan actualmente en otras tecnologías (es el caso de los programas de almacenamiento y borrado automático de imágenes y grabaciones ya incorporados a las CCTV), se aplican de manera dispersa en algunos Estados miembros que han desarrollado iniciativas sobre el uso de drones en relación con la protección de datos (nos referimos a la publicación de Guías por parte de las Autoridades de protección de datos o de Códigos de autorregulación adoptados voluntariamente por los operadores de drones) o, finalmente, están incluidas en el futuro Reglamento europeo (por ejemplo, las evaluaciones de impacto o la figura del delegado de protección de datos).

Por ello y a propósito de las novedades legislativas, creemos que el cambio normativo que se prepara en el doble nivel nacional y europeo será positivo. Por un lado, el proyecto de Real Decreto elaborado por el Ejecutivo español aunque regula con cautelas y numerosas restricciones las actividades autorizadas a los drones, atiende al estado actual de la tecnología e introduce seguridad jurídica en un ámbito todavía reglamentado con carácter temporal. Destacadamente, la nueva reglamentación contribuirá a garantizar los niveles adecuados de seguridad y protección física de las operaciones de drones y, entre otras cosas y por lo que aquí nos interesa, clarificará la determinación del sujeto responsable lo que es decisivo a los efectos de quién debe asegurar que el tratamiento de los datos y las obligaciones de custodia y conservación de los mismos y de los ficheros se realizan conforme a lo que imponen las normas en la materia. Por otro lado, el nuevo marco europeo en materia de protección de datos incluye mecanismos ya comentados que se adaptan a los retos que los drones civiles presentan para la protección de datos y que son insuficientemente cubiertos en las normativas nacionales. La aplicación escrupulosa de esta regulación contribuirá a atenuar las incertidumbres de los ciudadanos en relación con su intimidad y protección de datos. Estas garantías relativas a la privacidad deberían, además, ser tenidas en cuenta por los Estados miembros y la Unión Europea para incorporarlas explícitamente en el desarrollo de cualquier política sobre drones de uso civil.

Ambos aspectos son complementarios e indispensables para el desarrollo del sector. La seguridad y la protección física constituyen elementos clave para las operaciones de vuelo realizadas con drones aunque la aceptación social frente al uso de estos aparatos pasa, irrenunciablemente, por la garantía de los derechos fundamentales de los ciudadanos.

Title:

The emerging use of civilian drones in Spain. Legal status and impact on the right to data protection

Summary.

1. THE REVOLUTION OF DRONES. 2. SPANISH REGULATORY FRAMEWORK FOR DRONES. 2.1 Explanatory notes on the concept of drone. 2.2 Civilian uses of drones. 3. DATA PROTECTION IMPLICATIONS OF THE CIVILIAN USE OF DRO-

NES. 3.1 The legal treatment of data protection in the use of drones for public purposes. 3.2 Compliance with the principles of the Spanish Data Protection Act by the operator of a drone for private purposes. 4. PROPOSALS FOR A HARMONISED REGULATORY FRAMEWORK ON DATA PROTECTION AND THE CIVILIAN USE OF DRONES. 5. FINAL CONCLUSIONS

Resumen:

Los drones son una tecnología de moda y su uso civil ha comenzado a popularizarse en todo el mundo. España fue uno de los países pioneros en Europa en aprobar una legislación técnica sobre la materia con el objetivo de garantizar un alto nivel de seguridad. Ahora el foco de atención se centra en los retos que estas aeronaves pilotadas por control remoto plantean para la protección de datos y la intimidad. A la luz de las condiciones impuestas en la normativa española sobre protección de datos, nuestro estudio analiza las problemáticas que genera la explotación civil de los drones y presenta diversas propuestas doctrinales e institucionales para resolverlas.

Abstract:

Drones are a growth industry and their civilian uses are becoming popular all around the world. Spain was one of the first European countries to pass a technical regulation on RPAS with the aim of assuring a high security standard. Nowadays, attention is paid on the challenges that these technologies pose on privacy and data protection. In the light of the conditions imposed by the Spanish legislation on data protection, this paper analyses the concerns posed by the exploitation of civil drones and and looks at the major doctrinal and institutional attempts to address them.

Palabras clave:

drones, intimidad, protección de datos personales, LOPD, Reglamento General de Protección de Datos.

Key words:

RPA, privacy, personal data protection, Spanish Data Protection Act, General Data Protection Regulation.

