FACULTAD DE DERECHO

LA IRRUPCIÓN DE LOS DRONES Y EL DERECHO A LA INTIMIDAD: UNA APROXIMACIÓN NORMATIVA

Autor: Isabel García de Paredes Sánchez
5º E-5
Área de Mercantil

Tutor: Juan Francisco Falcón Ravelo

Madrid
Abril de 2020

ÍNDICE

ABREVIATURAS

AEPD – Agencia Española de Protección de Datos

ATO – Organización de Formación Aprobada

FAA – *Federal Aviation Administration*

Ibid – Indica que el trabajo que se cita es el mismo que el citado en la nota inmediatamente anterior, coincidiendo en autor, título y edición.

Id – Indica que el trabajo que se cita es el mismo que el citado en la nota inmediatamente anterior, coincidiendo en autor, título, edición y página.

Kg – Kilográmos

Km – Kilómetros

Km/h – Kilómetros por hora.

LOPD – Ley Orgánica de Protección de Datos

LOPD – Ley Orgánica de Protección de Datos

Nº - Número

NTIA – *National Telecommunications and Information Administration.*

RGPD – Reglamento General de Protección de Datos

TSA – *Transportation Secutiry Administration.*

vs. – Versus

Vol. – Volumen

LA IRRUPCIÓN DE LOS DRONES Y EL DERECHO A LA INTIMIDAD: UNA APROXIMACIÓN NORMATIVA

I. INTRODUCCIÓN

En la sociedad digitalizada en la que vivimos, la información se ha convertido en un bien preciado. Se calcula que este año unas seis mil millones de personas utilizarán *smartphones* y que habrá mas de cincuenta mil millones de aparatos que tengan una conexión activa a Internet. Todos ellos generan y comparten millones de terabytes de información personal de cada usuario[1].

Dentro de estos nuevos aparatos que generan y comparten datos, el papel de los drones ha crecido exponencialmente. Históricamente, los drones se han utilizado en el ámbito miliatr. El desarrollo que estos aparatos han tenido en el ámbito civil ha ido creciendo, al mismo tiempo que los drones se hacían más baratos de producir y de comercializar. Por menos de 100€ se pueden encontrar pequeños drones con tecnología básica en tiendas de juguetes o por Internet[2]. Por más de 100€ se pueden comprar drones profesionales con cámaras y sensores de alta calidad[3].

La realidad es que las posibilidades que tienen los drones en el ámbito civil se han multiplicado en los últimos años. No es complicado encontrar ejemplos de servicios que ya utilicen los drones para desarrollar la actividad profesional.

Desde la reconstrucción de escenas de crímenes, topografía, cinematografía y hasta para el ocio, los drones se han convertido en una parte del desarrollo tecnológico de la sociedad. Este desarrollo, sin embargo, no viene exento de problemas o de polémicas. Los drones pueden incluir numerosos instrumentos o dispositivos (cámaras de video,

---

[1] Cerveras Navas, L. "La primera en el peligro de la privacidad: La Unión Europea y la defensa del derecho fundamental a la protección de datos personales." *Boletín de la Academia Malagueña de Ciencias*, vol. 20, 2018, pp 9-17. Página 2.

[2] Para poder observar algunos ejemplos, diríjase a Amazon, donde se pueden encontrar drones con cámaras y control remoto de menos de 1kg por 40,49€ (referencia: Potensic Mini Drone para Niños con Cámara, RC Quadcopter 2.4G 6 Ejes - Altitude Hold, Modo sin Cabeza, Control Remoto, Ajuste de Ruta, FPV en Tiempo Real, 2 Baterías, A20W).

[3] Para poder observar algunos ejemplos, diríjase a Amazon, donde se pueden encontrar drones de 2 km por 439€ con cámaras 4K y autonomía y rango de hasta 4 km (referencia: HUBSAN Zino Pro GPS FPV Drone Plegable 4K Cámara 3 Ejes Cardán 4KM 23 Minutos App WiFi Control).

sistemas de geolocalización, sistemas de detección de dispositivos móviles, etc.) que pueden suponer una intromisión en el espacio privado de las personas, grabar imágenes, una videovigilancia, etc; en definitiva, una invasión del derecho a la protección de la imagen y la intimidad y datos de las personas y, en consecuencia, un ataque a sus derechos y libertades. Es por ello por lo que este trabajo versará sobre el uso de drones y la problemática que estos generan en relación con el derecho fundamental a la intimidad recogido en el artículo 18 de la Constitución española y al derecho a la protección de datos de las personas, contenido fundamentalmente en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de derechos digitales y en el Reglamento General de Protección de Datos (RGPD).

II. LOS DRONES

Antes de comenzar el desarrollo sobre el conflicto entre el uso civil de los drones y el derecho a la intimidad, es necesario, definir brevemente qué es un dron, cuál es su historia y los tipos de drones que se pueden encontrar actualmente en el mercado. Es necesario realizar esta primera aproximación para determinar cuáles son las verdaderas capacidades y ámbito de actuación de los drones para así poder identificar la amenaza que suponen, en su caso, desde el punto de vista del Derecho Privado de las personas.

En primer lugar, por lo que se refiere a su definición, la comunidad internacional identifica como drones a las *"aeronaves que vuelan sin un piloto a bordo y que pueden, o bien ser controladas plenamente por el piloto a través de control remoto, o bien estar programadas y ser completamente autónomas"*[4].

1. BREVE RESEÑA HISTÓRICA DE LOS DRONES

Los drones no son invenciones recientes, sino que tiene más de 100 años de historia. Los primeros artefactos no tripulados fueron probablemente los globos de aire caliente sin piloto, que datan de 1849[5]. Sin embargo, no son considerados drones principalmente porque su vuelo no podría ser controlado a distancia. Para poder encontrar el primer artefacto no tripulado que pueda asimilarse a la idea de un "dron" es necesario remontarse

[4] Real Decreto 1036/2017, de 15 de diciembre, por el que se regula la utilización civil de las aeronaves pilotadas por control remoto, y se modifican el 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 el Real Decreto 57/2002, de 18 de enero, por el que se aprueba el Reglamento de Circulación Aérea, preámbulo.

[5] Delgado, V., "Historia de los drones", El Dron

a la creación de las técnicas de control por radio, desarrolladas por primera vez por Nikola Tesla en 1898[6]. De los primeros vuelos que se realizaron con esta técnica, el más destacado fue el Hewitt-Sperry Automatic Airplane en 1917.

Durante el periodo de entreguerras se experimentó con el control por radio, transformando aviones de la Primera Guerra Mundial en drones. Alguno de los ejemplos más prominentes son el Larynx (1927), la Fairy Queen (1931) y el DH.82B Queen Bee. Se especula que el nombre actual de los drones proviene de este último avión, dado que "drone", en inglés, significa zángano[7] y "Queen Bee" abeja reina.

En la Segunda Guerra Mundial, y haciendo uso de los avances que se habían producido en el periodo de entreguerras, la Compañía Radioplane desarrolló y produjo más de 15.000 drones del modelo Radioplane OQ-2 para el ejército americano[8]. Se considera, por tanto, que este fue el primer dron que se produjo en masa en la historia.

Tras la Segunda Guerra Mundial, el uso de los drones comenzó a diversificarse. Además de para lanzar bombas, se comenzaron a utilizar para el reconocimiento aéreo. El primer dron en realizarlo fue el MQM-57 Falconer[9], que se creó en 1955. Se fabricaron más de 17.000 unidades y se llegaron a utilizar en más de 18 países.

Durante todo el siglo XX, el principal uso que se continuó dando a los drones fue el militar. En la Guerra de Vietnam, en la que el ejército americano utilizó los drones Ryan Firebee[10] y la CIA y el ejercito americano actualmente usan los drones MQ-1 Predator para reconocimiento y ataque. Se pueden volar de forma remota y a gran distancia, de forma que un piloto en una base en EE. UU. puede controlar a la perfección un dron que esté realizando alguna actividad en Oriente Medio. Se ha utilizado recientemente en Afganistán, Pakistán, Bosnia, Serbia, Irak, Yemen, Libia, Siria y Somalia[11]. Es muy útil para misiones en terreno poco accesible o que entrañe gran riesgo para las tropas, dado que puede llevar cámaras y otros sensores e incluso misiles. Además, también han sido

---

[6] Delgado, V., "Historia de los drones", El Dron

[7] *Ibid*

[8] *Ibid*

[9] Zaloga, S. J., "Unmanned aerial vehicles: robotic air warfare 1917-2007", Osprey Publishing, Oxford, 2008.

[10] Yenne, B., "Attack of drones: a history of unmanned aerial combat", Zenith Press, St Paul, 2004..

[11] Whittle, R., "Predator: the secret origins of the drone revolution", Henry Holt and Co, Nueva York, 2014.

utilizados para el control de fronteras, estudios científicos y para el control del estado de fuegos forestales activos[12].

Hasta el inicio del siglo XXI no se observa un uso masivo de los drones en ámbito civil. Este cambio se produce gracias al desarrollo de nuevos materiales ultraligeros y al abaratamiento de los costes de producción y comercialización[13].

2. TIPOS DE DRONES Y SUS PRINCIPALES CARACTERÍSTICAS

La primera distinción que hay que realizar es entre el dron en sí mismo (la plataforma) y el equipo añadido a él (los sensores o dispositivos incluidos o adheridos a la plataforma). En el contexto del uso civil, los drones se pueden considerar unas plataformas volantes a las que se pueden adaptar diferentes sensores para realizar tareas muy diversas.

2.1. Tipos de plataformas

La característica más notable es lo que se denomina el tipo de plataforma. La importancia de esta característica está en el hecho de que los diferentes tipos de plataformas pueden aceptar unos tipos diferentes de sensores o dispositivos y se pueden utilizar para unos usos diferentes..

La mayoría de los drones existentes se pueden clasificar fundamentalmente en dos tipos, que son los sistemas de ala fija y los sistemas multirrotor. El término ala fija se utiliza principalmente en la industria de la aviación para definir las aeronaves que utilizan alas fijas y estáticas en combinación con la velocidad del aire hacia adelante para generar elevación[14]. Algunos ejemplos de este tipo de aviones son las cometas, los diferentes tipos de planeadores como parapentes o alas delta y, por supuesto, los aviones tradicionales.

Por otro lado, los sistemas multirotor se componen por un conjunto de los rotores, que son alas giratorias que generan elevación. El ejemplo más claro son los helicópteros tradicionales, que pueden tener uno o varios rotores. Los drones que utilizan este sistema de elevación están equipados con varios rotores[15]

---

[12] Whittle, R., "Predator: the secret origins of the drone revolution", Henry Holt and Co, Nueva York, 2014

[13] Vergouw, B., Nagel, H., Bondt, G y Custers, B. "Drone Technology: Types, Payloads, Applications, Frequency Spectrum Issues and Future Developments", en Custers, B. (Ed), The Future of Drone Use: Opportunities and Threats From Ethical and Legal Perspectives, Springer, Amsterdam, Paises Bajos, 2016. Página 10.

[14] *Ibid,* Página 24.

[15] Vergouw, B., Nagel, H., Bondt, G y Custers, B. "Drone Technology: Types, Payloads, Applications,

En lo que respecta al vuelo, y debido a la ausencia de un piloto, los drones siempre tienen un cierto nivel de autonomía[16]. Una distinción importante dentro del concepto de autonomía es la diferencia entre sistemas automáticos y autónomos. Un sistema automático es un sistema completamente preprogramado que puede realizar una operación pre-programada por sí mismo. Por otro lado, los sistemas autónomos pueden hacer frente a situaciones inesperadas mediante el uso de unas reglas para ayudarles a tomar decisiones. Los sistemas automáticos no pueden ejercer esta "libertad de elección".

Hay principalmente cuatro fuentes de alimentación[17]: keroseno, para drones pesados y que requieren de mucho tiempo de funcionamiento, baterías, usados para drones pequeños y ligeros y paneles solares, aún no muy funcionales pero que se están desarrollando actualmente.

2.2. Tipos de sensores

Para poder ejecutar el plan de vuelo establecido por el piloto, los drones necesitan de múltiples sensores. Estos sensores tienen una función esencial en el uso del dron, que es recoger la información, que puede ser procesada y analizada directamente o a través de la ayuda de un programa de software. Los sensores son la parte más importante del dron, ya que es la que aporta verdadera funcionalidad al aparato.

Los sensores se pueden clasificar fundamentalmente en tres categorías, sensores activos, sensores pasivos y sensores fundamentales para el vuelo[18]. Los primeros se caracterizan por ser aparatos que miden cómo se comporta la radiación que ellos mismos emiten. Es decir, generan pulsos, que lanzan al espacio sobre el que vuelan. Este pulso rebota contra las superficies contra las que choca, permitiendo al dron medir este rebote y confeccionar un mapa preciso del espacio. El principal problema que acarrea es que suelen ser sensores de gran tamaño, que requiere de plataformas muy grandes para transportarlos. En consecuencia, en general sólo se utilizan para fines comerciales muy concretos como por

---

Frequency Spectrum Issues and Future Developments", en Custers, B. (Ed), The Future of Drone Use: Opportunities and Threats From Ethical and Legal Perspectives, Springer, Amsterdam, Paises Bajos, 2016. Página 24.

[16] *Ibid*, página 25.

[17] "Todas las partes de los drones explicadas al detalle", Esenziale

[18] Vergouw, B., Nagel, H., Bondt, G y Custers, B. "Drone Technology: Types, Payloads, Applications, Frequency Spectrum Issues and Future Developments", en Custers, B. (Ed), The Future of Drone Use: Opportunities and Threats From Ethical and Legal Perspectives, Springer, Amsterdam, Paises Bajos, 2016. Página 30.

ejemplo la topografía[19].

Los segundos son los sensores pasivos[20]. Al contrario que los activos, no registran radiación producida por ellos mismos, sino la emitida por los propios objetos. Son los sensores más habituales dentro de los drones civiles y algunos de los más comunes pueden ser las cámaras fotográficas, las cámaras de vídeo, las infrarrojas o las térmicas. Suelen ser de tamaño muy reducido y consumen muy poca energía, por lo que pueden ser transportadas por plataformas más pequeñas y transportadas a mucha más distancia, con un consumo de energía mucho menor.

El Grupo de Trabajo del artículo 29, un grupo independiente creado por la Comisión Europea encargado de cuestiones sobre protección de datos y que ayudó crear la legislación actual sobre este asunto, divide estos sensores pasivos en tres categorías[21]. La primera de ellas son los equipos de grabación, como pueden ser las cámaras arriba descritas. El segundo son los equipos de detección, como los sensores optoeléctricos o los radares de apertura sintéticos, que hasta permiten conocer lo que se encuentra tras paredes de hormigón[22]. Los terceros son los equipos de radiofrecuencia, que son antenas que pueden localizar puntos de Wifi o la localización de teléfonos móviles encendidos.

Cabe subrayar, por tanto, que los datos que los drones pueden recopilar con este tipo de sensores distan mucho de ser solo imágenes fotográficas o videos. A través de los sensores se pueden obtener datos que van más allá de lo que percibe el ojo humano, como por ejemplo los rayos ultravioleta o infrarrojos. Todas estas funcionalidades se pueden, sin embargo, llevar más allá y combinar en un mismo sensor, dando lugar a las denominadas cámaras multiespectrales[23]. Este tipo de sensor, diseñado específicamente para el uso de drones, posee cinco lentes que se corresponden cada una con bandas diferentes de espectros de luz. Las lentes más comunes que suelen incorporar son cuatro periféricas (una roja, una verde, una azul, otra de infrarrojo cercano NIR) y otra lente

---

[19] "Todas las partes de los drones explicadas al detalle", Esenziale

[20] *Id.*

[21] Grupo de Trabajo sobre el Artículo 29, "Informe 01/2015 sobre privacidad y protección de datos relacionados con la utilización de Drones", Comisión Europea, 2015. Páginas 6 y 7.

[22] i Marquès, M. C., "Drones recreativos y responsabilidad civil (Tras la reforma de 2017)", Revista de Derecho Civil, vol. 6, nº 1, 2019, pp. 297-333. Página 322.

[23] Kharuf-Gutierrez, S., Hernández-Santana, L., Orozco-Morales, R., Aday Díaz, O., y Delgado Mora, I., "Análisis de imágenes multiespectrales adquiridas con vehículos aéreos no tripulados", Ingeniería Electrónica, Automática y Comunicaciones, vol. 39, nº 2. Páginas 79-91.

central, que captura imágenes RGB compuestas.

No hace falta ir muy lejos en el tiempo para ver como este tipo de cámaras que incorporan la funcionalidad de varios sensores han sido utilizados de forma masiva. En la reciente lucha contra la crisis sanitaria generada por el COVID-19, tan de actualidad en estos momentos, el gobierno chino[24] utilizó drones con cámaras infrarrojas para medir la temperatura de todos los ciudadanos chinos, tanto dentro de edificios como por la calle. Si alguno de ellos tenia fiebre, eran reconocidos por el dron a través de la cámara de video y un software de reconocimiento facial y marcados. Los datos eran enviados a las autoridades, que pasaban a visitar al ciudadano en cuestión para forzarlo a ir a un hospital o a aislamiento.

Por último, es necesario mencionar los sensores que son necesarios para que las plataformas puedan volar de forma estable y ejecutar las funciones que los pilotos han programado o quieren realizar. Son fundamentalmente[25] el GPS, el acelerómetro, el altímetro, el giroscopio y la brújula. Este tipo de sensores recogen datos, en general, que afectan al propio funcionamiento del dron, como puede ser la altitud a la que vuela, la aceleración estática y dinámica, los ángulos de ubicación del dron… no recogen y procesan información sobre lo que ocurre en el espacio en el que vuelan, sino que sirven para estabilizar el vuelo y permiten que los dos primeros tipos de sensores recaben la información necesaria.

A la vista de las funcionalidades descritas, no resulta difícil imaginar la cantidad de ocasiones y escenarios en los que la mera utilización de los drones puede chocar con derechos a la intimidad o protección de los datos de las personas y en ello centraremos nuestro estudio a continuación.

Con esta descripción de los diferentes sensores queda claro que la recopilación de datos que pueden llevar a cabo los drones va mucho más allá de la simple toda de imágenes fotográficas o de video. La intromisión en la vida privada de las personas es mucho más profunda. Por ejemplo, gracias a los diferentes sensores que se pueden incorporar, se puede programar a un dron para que capte una señal wifi de un móvil. Una vez que la

---

[24] De la Cal, L., "Tecnología china contra el coronavirus: de drones termómetro a apps que se chivan si te pones malo" El Mundo, 13 de marzo de 2020 (disponible en: https://www.elmundo.es/tecnologia/2020/03/13/5e68a08121efa08f5b8b475c.html; última consulta 08/04/2020).

[25] "Todas las partes de los drones explicadas al detalle", Esenziale

tenga localizada, puede seguirla y trazar un mapa preciso de todos los lugares a los que haya ido la persona que porte el móvil que emite la señal. No solo eso. Algunos drones también tienen la capacidad de reconocer figuras a través de las paredes de hormigón y grabar los movimientos que se hagan, por ejemplo, en una oficina. Pueden detectar huellas de calor y medir la temperatura de cualquier persona.

Los datos personales que pueden captar los drones, en resumen, no son solo nuestras imágenes. También pueden recopilar datos de la ruta que llevamos, los lugares concretos que hemos visitado, las personas con las que nos hemos encontrado, la temperatura corporal y hasta lo que hacemos en la intimidad de nuestra casa u oficina. Es por ello por lo que es fundamental tener una normativa estricta y clara sobre que datos se pueden captar, cómo y hasta que punto pueden distribuirse.

III. DERECHO A LA INTIMIDAD Y A LA PRIVACIDAD

El derecho a la intimidad y a la privacidad de las personas es un derecho básico para el desarrollo en libertad de las sociedades, ya que, como apunta Leonardo Cerveras Navas, director de la oficina del Supervisor Europeo de Protección de Datos, *"el único comportamiento humano que es verdaderamente libre es el que se hace en privado, lejos de la mirada de los demás"*[26]. Por tanto, con el derecho a la intimidad se protege la necesidad de las personas de tener un espacio propio y privado en el que desarrollar su vida. Dentro de este derecho, el derecho a la protección de los datos personales se configura como un pilar fundamental, por el cual las personas no solo tienen derecho a protegerse de las miradas indiscretas del mundo, sino también a controlar y decidir qué hacer con la información que el mundo dispone sobre ellos.

1. ACLARACIÓN TERMINOLÓGICA

Intimidad y privacidad se suele utilizar de forma habitual como sinónimos, tanto por juristas, como por los medios de comunicación, a pesar de que terminológicamente no significan lo mismo. Lo privado se refiere, según juristas como Díaz Rojo[27], a privar, concepto muy relacionado con la propiedad privada o, lo que es lo mismo, lo contrario a

[26] Cerveras Navas, L., "La Primera en el Peligro de la Privacidad: la Unión Europea y la Defensa del Derecho Fundamental a la Protección de Datos Personales" Discurso de ingreso como Académico Correspondiente, Bruselas, Bélgica, 2017.

[27] Díaz Rojo, J.A., "Privacidad: ¿neologismo o barbarismo?", *Consejo Superior de Investigaciones Cientificas*

lo público. La intimidad es, por otra parte, un concepto que se refiere a aspectos más profundos del ser humano, como pueden ser los sentimientos, la ideología o el pensamiento. Ambos conceptos, a un nivel semántico, son diferentes y no deben de utilizarse como sinónimos.

En el ámbito del Derecho y, en especial, en el ámbito de la protección de datos, los citados términos tienden a utilizarse como sinónimos. Pero incluso en el mundo del Derecho existen diferencias entre los que se entiende en el sistema del *common law* sobre el *right to privacy*, o el derecho a la privacidad, mucho más unido a la privacidad entendida como propiedad privada, por contraposición a lo público, y la concepción europea sobre el derecho a la intimidad. Por tanto, y para ser absolutamente correctos en la utilización de los términos en el desarrollo del presente trabajo, utilizaremos derecho a la privacidad para referirnos al sistema americano y el derecho de intimidad para referirnos al sistema continental o europeo. Es necesario puntualizar, sin embargo, que tanto la legislación como la jurisprudencia tiende a utilizar estos términos como sinónimos.

2. BREVE APUNTE HISTÓRICO SOBRE EL DERECHO A LA INTIMIDAD

El derecho a la intimidad o privacidad se reconoce como uno de los derechos innatos de las personas. Fue incluido dentro de la primera generación de derechos en ser recogido por las Declaraciones de Derechos del siglo XVIII, pero, paradójicamente, en ningún momento fue regulado o denominado derecho de intimidad o privacidad. Este derecho se encontraba subsumido en el derecho a la propiedad privada en general[28].

El desarrollo filosófico, ético y moral sobre la individualidad y la necesidad de mantener la intimidad, alejada del foco privado, tuvo gran desarrollo durante el siglo XIX. A pesar de ello, el desarrollo doctrinal jurídico de este derecho de forma concreta y separada de la propiedad privada surge en EEUU, con la obra del juez Thomas McIntyre Cooley *"Elements of Torts"*[29]. En el se nombra por primera vez en el ámbito jurídico el derecho de ser dejado solo, en paz (*"the right to be left alone"*). Tras este trabajo, el desarrollo en profundidad lo realizaron tan solo cinco años más tarde otros dos autores americanos, Brandeis y Warren, en su obra *"The right to privacy"*[30]. De forma general, la publicación

[28] Rodríguez, J. P., "El proceso de constitucionalización de una exigencia ética fundamental: el derecho a la intimidad", *Revista del Instituto Bartolomé de las Casas*, 1994, pp- 363-392. Página 2.

[29] McIntyre, T.C., "The elements of Torts", Callaghan and Company, 1895.

[30] Warren, S.D. y Brandeis, L.D., "The Right to Privacy", *Harvard Law Review*, vol. 4, 1890. Página 193.

de esta obra se suele marcar como la fecha de nacimiento del derecho a la privacidad en EEUU. Esta obra no surge de la nada, sino que nace por las necesidades que comenzaban a aflorar en la sociedad de la época. El derecho a la privacidad es una respuesta a la necesidad de protección de las personas frente a la prensa, que en aquella época comenzaba a tener relevancia dentro de la sociedad americana. La culminación de este derecho como autónomo lo da la sentencia de Pavesich v. New England Life Insurance Company del Tribunal Supremo de EEUU en 1905[31]. Este derecho continuó desarrollándose, pero siempre fuera de los derechos con reconocimiento constitucional. En consecuencia, las violaciones a la privacidad se entienden que quedan sujetas a responsabilidad y por tanto a la compensación de la victima[32].

La preocupación en Europa sobre el derecho a la intimidad surge principalmente al inicio del siglo pasado, con el nacimiento de la sociedad de la información y la difusión masiva de los datos, al igual que en Estados Unidos. Como indica Jesús Rodríguez en su obra "El proceso de Constitucionalización de una Exigencia Ética Fundamental: el Derecho a la Intimidad", *"este paralelismo no es casual, ya que en una sociedad tecnificada, con sofisticados sistemas de difusión, ya sean de forma audiovisual o escrita, la persona humana se encuentra más inerme que nunca frente a posibles abusos en la transmisión de informaciones que afectan a su persona"*[33]. Esta necesidad comienza a ser imperante con el desarrollo exponencial de la tecnología, pero no es hasta la Constitución Portuguesa de 1976, seguida por la Constitución Española de 1978, cuando este derecho encuentra una regulación formal como derecho fundamental. El desarrollo desde ese momento ha sido vertiginoso, principalmente por el estallido de las nuevas tecnologías, en particular Internet, en las que los datos y la intimidad de las personas son fácilmente violables. Por último, es necesario mencionar que este derecho está ya consolidado en toda Europa, ya que lo recoge en la Carta de Derechos Fundamentales de la Unión Europea en su artículo 7[34].

---

[31] Kharuf-Gutierrez, S., Hernández-Santana, L., Orozco-Morales, R., Díaz, A., y Kent Jr, M. B., "Pavesich, Property and Privacy: The Common Origins of Property Rights and Privacy Rights in Georgia", *J. Marshall LJ*, vol. *2*, nº 1, 2009.

[32] González Porras, A. J. "Privacidad en internet: los derechos fundamentales de privacidad e intimidad en internet y su regulación jurídica. La vigilancia masiva" Tesis, Universidad de Castilla La Mancha, 2015. Página 76

[33] Rodríguez, J. P., "El proceso de constitucionalización de una exigencia ética fundamental: el derecho a la intimidad", *Revista del Instituto Bartolomé de las Casas*, 1994, pp- 363-392. Página 2.

[34] Carta de los Derechos Fundamentales de la Unión Europea, DOUE núm. 83, de 30 de marzo de 2010,

3. DERECHO A LA INTIMIDAD Y LAS NUEVAS TECNOLOGÍAS

Nuestra vida actualmente se encuentra, de forma irremediable, entrelazada con la tecnología, a la que confiamos todos nuestros datos. A través del teléfono móvil manejamos los datos del banco, realizamos una gran parte de nuestras compras, consumimos entretenimiento y hasta consultamos con los médicos. Utilizamos las bases de datos para realizar trabajos y nos relacionamos con la administración a través de medios telemáticos. Nuestras relaciones sociales se desarrollan a través de redes sociales y aplicaciones de mensajería. Al utilizar todas estas aplicaciones, de forma consciente o inconsciente, proporcionamos nuestros datos a la red.

Es en este punto en el que choca el derecho a la intimidad con las nuevas tecnologías y en el que surge, amparada por él, la obligación de la protección de datos de las personas. Esta protección consiste en *"la prerrogativa de la persona para disponer de la información sobre sí misma que exista en los registros o bases de datos, a fin de que esa información sea veraz, íntegra, actualizada, no intrusiva, y con las garantías de seguridad y de uso conforme a la finalidad para la que fue proporcionada"*[35]. En otras palabras, es el derecho que cubre la posible utilización por parte de terceros de datos personales sin el debido consentimiento.

La primera ley que surge sobre este ámbito en Europa es en Alemania, sobre la protección de los datos informáticos[36], en 1970. Al mismo tiempo, en Estados Unidos se promulgó en 1974 el *Privacy Act*, sobre la protección de datos en relación con las ciencias computacionales, que se desarrolló de forma más concreta en la *Electronic Communications Privacy Act* en 1985[37]. En la Unión Europea, del derecho negativo de la intimidad surge un derecho positivo sobre el tratamiento de los datos, a través del artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea[38].

---

páginas 389 a 403.

[35] González Porras, A. J. (2016). Privacidad en internet: los derechos fundamentales de privacidad e intimidad en internet y su regulación jurídica. La vigilancia masiva, página 199.

[36] Aguilera, A. T. (2002). La protección de datos en la Unión Europea: divergencias normativas y anhelos unificadores. Edisofer, página 28.

[37] González Porras, A. J. "Privacidad en internet: los derechos fundamentales de privacidad e intimidad en internet y su regulación jurídica. La vigilancia masiva" Tesis, Universidad de Castilla La Mancha, 2015. Página 199.

[38] Carta de los Derechos Fundamentales de la Unión Europea, DOUE núm. 83, de 30 de marzo de 2010, páginas 389 a 403

Como se puede observar, el derecho de autogestión de los datos es relativamente nuevo, y vienen ligado a la aparición de Internet y las nuevas tecnologías. En este contexto, es claro que el uso de drones puede generar problemas en este ámbito. Los terceros pueden ser conscientes de que esta información está siendo recopilada, como por ejemplo en los casos en los que el dron se utiliza como herramienta cinematográfica. Pero también puede no ser conscientes de que están siendo observados por diferentes objetivos. Durante los vuelos del dron, como, por ejemplo, de vigilancia, estos pueden captar imágenes de personas caminando por la calle o tomando el sol en las terrazas. Todo ello sin mencionar la posibilidad de que directamente se utilice esta tecnología para de forma consciente violar la privacidad de las personas. En ese contexto, los operadores de drones que registren o procesen imágenes, vídeos, sonidos y, en general, cualesquiera datos personales relacionados con una persona identificada o identificable en nuestro país están sujetos no solo a la normativa reguladora del uso de drones, sino también a la normativa de protección de datos personales en general.

IV. LEGISLACIÓN ESPAÑOLA

1. LEGISLACIÓN SOBRE EL USO DE DRONES

1.1. Uso profesional

La regulación en España del uso de drones es tanto europea como nacional. Se recoge principalmente en la Ley 21/2003, de 7 de julio, de Seguridad Aérea[39], Reglamento (UE) del aire[40], el Real Decreto 57/2002[41] y el Real Decreto 1036/2017[42] que deroga la Ley 18/2014, de 15 de octubre, de aprobación de medidas urgentes para el crecimiento, la competitividad y la eficiencia[43].

[39] Ley 21/2003, de 7 de julio, de Seguridad Aérea, BOE núm. 162.

[40] Reglamento (UE) número 923/2012 de la Comisión, de 26 de septiembre de 2012, por el que se establecen el Reglamento del aire y disposiciones operativas comunes para los servicios y procedimientos de navegación aérea

[41] Real Decreto 57/2002, de 18 de enero, por el que se aprueba el Reglamento de Circulación Aérea, BOE núm. 17, páginas 2449 a 2450.

[42] Real Decreto 1036/2017, de 15 de diciembre, por el que se regula la utilización civil de las aeronaves pilotadas por control remoto, y se modifican el 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 el Real Decreto 57/2002, de 18 de enero, por el que se aprueba el Reglamento de Circulación Aérea. BOE número 216, de 29 de diciembre de 2017, páginas 129609 a 129641.

[43] Ley 18/2014, de 15 de octubre, de aprobación de medidas urgentes para el crecimiento, la competitividad y la eficiencia. BOE número 252, de 17 de octubre de 2014.

La Ley 18/2914 recogía el marco específico en el que se permite el vuelo de los drones en el espacio aéreo español. Antes de esta ley no existía ninguna regulación concreta sobre el uso de los drones, lo que creaba una gran inseguridad jurídica. El uso de los drones ya estaba extendido a lo largo de la sociedad civil y, de acuerdo con el preámbulo de la propia ley, era necesario crear un marco de actuación para que tanto los pilotos como la sociedad en general pudiera disfrutar de los avances tecnológicos en un espacio de seguridad. En esta ley se regulaba en su artículo 50 el uso de las aeronaves civiles pilotadas por control remoto.

Este artículo queda derogado, y con ello todo el marco jurídico que establecía para los drones, por el Real Decreto 1036/2017.

Por lo que se refiere al ámbito objetivo de aplicación de este Real Decreto, el mismo regula los drones de uso civil profesional que pesan menos de 150 kg y que no pertenecen a las Fuerzas y Cuerpos de Seguridad del Estado (artículo 2.1).

Se excluyen expresamente de la regulación de este Real Decreto (artículo 2.2.) los drones de uso militar, de exhibición aérea, de actividades deportivas, de uso recreativo o de competición y los drones de juguete.

De acuerdo con el Real Decreto 1036/2017para poder volar un dron incluido dentro del ámbito objetivo de aplicación del referido Real Decreto antes apuntado, es necesario que el piloto sea mayor de edad, disponga de un certificado médico en vigor concreto para drones y que disponga de los conocimientos aeronáuticos suficientes. Para demostrar el conocimiento se puede, o bien tener una licencia de piloto, o estar en posesión de un certificado de la Organización de Formación Aprobada (ATO). Estas certificaciones se conceden con limitaciones, de forma que cada certificación permite volar unos drones determinados, con unas condiciones concretas (altura, distancia, condiciones climatológicas…). Esta certificación por si sola no permite el uso profesional de un dron. Para poder ejercer la profesión es necesario convertirse en un operador de vuelos profesional habilitado, o trabajar como asalariado para uno.

Para ser un operador de vuelos profesional es necesario tener una habilitación emitida por la Agencia Estatal de Seguridad Aérea (artículo 39 del Real Decreto 1036/2017). Para ello, es necesario entregar documentación concreta, como el seguro de responsabilidad civil, un manual de medidas de seguridad para las operaciones o un programa de mantenimiento de la aeronave. Esta habilitación permite realizar trabajos aéreos, que son

todos aquellos en los que no se vuela sobre aglomeraciones de edificios o personas, de día y con buenas condiciones meteorológicas, dentro del alcance visual del piloto y a no más de 120 metros de altura. Si se quieren realizar tareas más complejas, como el vuelo nocturno, sobre personas, o sobre edificios es necesario solicitar además autorizaciones extra para cada operación, en las que hay que demostrar que el piloto que va a llevar a cabo la operación tiene los conocimientos suficientes.

En cualquier caso, se debe de mantener una distancia mínima recogida el artículo 24 del Real Decreto con lugares utilizados para el aterrizaje y despegue de las aeronaves tripuladas.

Es necesario mencionar que la regulación para las operaciones de vuelo profesional con drones es muy minuciosa. Este hecho tiene, bajo mi punto de vista, consecuencias positivas y negativas. Por un lado, una regulación excesiva impide que muchas personas con ganas de dedicarse profesionalmente a los drones puedan acceder a esta profesión. El problema no es solo que tenga que superar muchos hitos para poder llegar a ser piloto y operador, sino que, además, cada uno de ellos conlleva una inversión económica que puede no estar al alcance de muchas personas.

Por otro lado, esta regulación prioriza la seguridad. Los drones, a pesar de que se consideren inofensivos, no son juguetes. Pueden provocar graves daños materiales y personales si no se controlan con prudencia. Por ello, el hecho de que los pilotos y operadores tengan que estar muy preparados para realizar una operación concreta hace que el riesgo de accidentes se reduzca. Por tanto, es necesario encontrar un punto intermedio de equilibrio entre ambos extremos. La legislación del uso de drones tiene que ser lo suficientemente protectora como para evitar en la medida de lo posible accidentes, pero lo suficientemente abierta como para no impedir el acceso a una nueva profesión a jóvenes sin grandes recursos.

1.2. Uso recreativo

El marco legal del uso recreativo de los drones es muy diferente del uso profesional. A pesar de que en el artículo 2.2. del Real Decreto 1036/2017 se indique que no regula los drones de uso recreativo, sí que éstos se incluyen en su disposición adicional segunda y tercera.

Para poder realizar un análisis preciso de cómo se regula el uso de drones con fines recreativos, hay que realizar una distinción entre los drones que realicen actividades

deportivas, recreativas, de competición y de exhibición, los aeromodelos, del uso recreativo de aeronaves de juguete. Esta clasificación que realiza el Real Decreto en el artículo 2 se corresponde con las diferencias entre los aeromodelos y las aeronaves de juguete. Las aeronaves de juguete son aquellas que están diseñadas para ser utilizadas por menores de 14 años para el juego. Al ser un juguete, se debe de aplicar la legislación concreta para ellos. Cabe remarcar que, para que cumpla con los requisitos, su fin tiene que ser un juguete, no un dron con funcionalidad plena y que pueda transportar sensores. Por tanto, en ningún caso pueden ser aparatos muy potentes, que tengan grandes baterías, o autonomía, con buena calidad de video y que resistan mucho tiempo en vuelo en el exterior. Esto hace que no sean aparatos muy útiles en lo que respecta a la recogida de datos[44].

Por otro lado, los aeromodelos son aeronaves pequeñas, que no superen en ningún caso los 150 kilogramos de peso y que puedan mantener el vuelo en la atmósfera. Por tanto, los aeromodelos se asimilan perfectamente a drones funcionales con capacidad para poder realizar vuelos estables al aire libre. La Agencia Europea de Seguridad Aérea ha aceptado esta similitud, debido a que gracias a los desarrollos tecnológicos es prácticamente imposible distinguir una de otra. Es por ello por lo que ha sometido a ambos a la misma regulación. Un ejemplo de esto es la Orden ETU/1033/2017, de 25 de octubre, por la que se aprueba el cuadro nacional de atribución de frecuencias[45].

Mientras que el uso de este tipo de drones para fines deportivos o de exhibición sí que está regulado por la normativa que establezca la Federación o club que los opere, el uso puramente recreativo se encuentra escasamente regulado[46]. El legislador, sin embargo, sí que ha impuesto una serie de limitaciones[47]. En primer lugar, deben de volar a una distancia mínima de 8 km de cualquier aeropuerto y siempre dentro del área de alcance visual del piloto y con una altura máxima de 120 metros. Los drones tienen que ir debidamente identificados en cualquier circunstancia. Además, solo pueden volar de día

---

[44] i Marquès, M. C., "Drones recreativos y responsabilidad civil (Tras la reforma de 2017)", *Revista de Derecho Civil*, vol. 6, nº 1, 2019, pp. 297-333. Página 304.

[45] Orden ETU/1033/2017, de 25 de octubre, por la que se aprueba el cuadro nacional de atribución de frecuencias, BOE núm. 259, de 27 de octubre de 2017, páginas 103115 a 103478.

[46] i Marquès, M. C., "Drones recreativos y responsabilidad civil (Tras la reforma de 2017)", *Revista de Derecho Civil*, vol. 6, nº 1, 2019, pp. 297-333. Página 306.

[47] "¿Qué podemos hacer con un dron?", *Agencia Estatal de Seguridad Aérea.*

y con buenas condiciones meteorológicas y nunca sobre aglomeraciones de edificios o personas. Esta última limitación no se tiene que respetar si el dron pesa menos de 250 gramos y vuele a una altura máxima de 20 metros. Esta limitación tiene especial sentido, ya que a día de hoy es imposible incorporar ningún sensor que pese tan poco. Igualmente, si el dron sufre algún accidente los daños que puede causar son mínimos.

Existe una gran diferencia entre la extensa regulación a la que se someten los pilotos de uso profesional y la poca regulación para los aficionados, especialmente en lo que se refiere a la formación de los pilotos. El hecho de que un piloto aficionado pueda volar sin ningún tipo de formación o habilitación prácticamente en las mismas condiciones que un piloto profesional con la habilitación más básica es, como mínimo, sorprendente. Como ya se ha mencionado anteriormente, los drones pueden ocasionar graves perjuicios y permitir que se piloten sin ninguna experiencia genera un riesgo.

2. LA CAPTACIÓN DE DATOS POR LOS DRONES

En el uso de drones y el tratamiento de los datos que recoge, es necesario respetar todos los preceptos legales correspondientes, no solo los que indican cómo y dónde se puede volar. Por tanto, todos los datos que los drones recogen durante su uso también tienen que estar acorde a la legislación nacional y europea, tanto en el momento de captación o tratamiento, como en momentos posteriores de procesamiento.

La protección del derecho a la intimidad y la normativa de protección de datos está íntimamente ligada. Cuando la vulneración del derecho a la intimidad implica la captación o tratamiento de datos personales se está vulnerando también la normativa de protección de datos. Es por ello por lo que a continuación se realizará un análisis conjunto de ambos preceptos.

Los drones son aparatos que pasan muy desapercibidos. Suelen ser pequeños, en general no hacen ruido, y tienen la capacidad de llegar a lugares recónditos y grabar con detalle[48]. Por ejemplo, un dron puede sobrevolar a 20 metros sobre el suelo y grabar lo que sucede dentro de una casa a través de las ventanas, a pesar de que el edificio sea alto. Igualmente, puede sobrevolar balcones y terrazas y grabar lo que allí acontece. Cabe, por tanto, que con estas acciones se esté produciendo una intromisión ilegítima con el derecho a la

[48] Cavoukian, A., "Privacy and drones: Unmanned aerial vehicles", Ontario: Information and Privacy Commissioner of Ontario, Ontario, Canada, 2012. Página 21.

intimidad de la persona que está siendo grabada en este momento y una vulneración de la normativa sobre protección de datos.

Cabe recordar en este contexto que un dato personal desde un punto de vista legal comprende "*toda información sobre una persona física identificada o identificable*"[49]. Por tanto, "dato personal" a efectos de su protección legal es cualquier información (incluso aunque no sea del todo completa) que pueda llevar a la identificación precisa de una persona. Por ejemplo, la información recogida por un dron gracias al seguimiento de una señal wifi de un móvil es un dato personal, ya que puede permitirnos saber, con el correspondiente cruce de información adicional, quién es la persona en cuestión y dónde se encontraba a una hora concreta y en un día determinado.

En España la protección de datos se regula por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de los Derechos Digitales[50] (LOPD), el Reglamento (UE) General de Protección de Datos[51] (RGPD) y la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo[52].

Esta ley consta de 10 títulos, que se extienden a lo largo de 97 artículos junto con 22 disposiciones adicionales, 6 disposiciones transitorias, 1 derogatoria y 16 finales. A lo largo de todo el articulado no hay ni una sola mención a los datos recogidos por los drones. Esto no significa, sin embargo, que esta legislación no se pueda aplicar a su uso. Es más, el artículo 26 del Real Decreto 1036/2017 establece que todo aquel que haga uso de drones tiene que garantizar el cumplimiento de la legislación sobre protección de datos[53]. Por tanto, siempre que un dron utilice sensores capaces de recopilar de datos de

---

[49] Agencia Española de Protección de Datos, "Drones y Protección de Datos", *Agencia Española de Protección de Datos*. Página 4.

[50] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, «BOE» núm. 294, de 6 de diciembre de 2018, páginas 119788 a 119857.

[51] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, Diario Oficial de la Unión Europea

[52] Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo

[53] Real Decreto 1036/2017, de 15 de diciembre, por el que se regula la utilización civil de las aeronaves pilotadas por control remoto, y se modifican el 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 el Real Decreto 57/2002, de 18 de enero, por el que se aprueba el Reglamento de

carácter personal, como por ejemplo cámaras de video, termográficas, de visión nocturna, escáneres 3D, sistemas de detección de dispositivos móviles… Cabe mencionar que la simple grabación de imágenes de video que queden almacenadas en una memoria, tanto externa como de la propia cámara constituye un tratamiento de datos personales automatizado según la justicia europea[54].

La regulación de la protección de datos europea y española establecen una serie de obligaciones generales que se tienen que respetar en todo momento. Estas obligaciones no están recogidas expresamente en la legislación sobre drones, y operan como principios generales.

2.1. Principios generales

Todos los drones que recojan datos tienen que seguir unas obligaciones generales que son cuatro, (i) uso legitimo y proporcionado del dron, (ii) minimización de datos, (iii) consentimiento y (iv) conservación de datos. En un primer lugar se explicarán estos principios, y se relacionarán con la "Guía sobre Drones y Protección de Datos"[55], un documento creado por la Agencia Española de Protección de Datos (AEPD) para orientar a los operadores sobre cuales son sus obligaciones en el tratamiento de datos. Esta guía divide las recomendaciones según el tipo de operación que se realiza. Por un lado, se encuentran todas las actividades cuya finalidad es de por sí la recopilación de datos, y por otro, aquellas que a priori no se incluye el tratamiento de datos. En este último caso, cabe una nueva subclasificación, en las actividades en las que no existe el riesgo de tratamiento de datos, y las actividades que si que tienen este riesgo[56].

En lo que respecta a las operaciones que no incluyen un tratamiento de datos personales, es necesario mencionar que son extremadamente infrecuentes. Como ya se ha esbozado a lo largo del trabajo, es claro que hasta los drones más básicos vendidos en cualquier plataforma online o en tiendas físicas llevan cámaras de video para pilotarlos. En este tipo

---

Circulación Aérea. BOE número 216, de 29 de diciembre de 2017, páginas 129609 a 129641.

[54] Sentencia del Tribunal de Justicia de la Unión Europea (Sala Segunda) de 14 de febrero de 2019, asunto C-345/17, Sergejs Buivids con la intervención de la Agencia Estatal de Protección de Datos de Letonia (ECLI:EU:C:2019:122).

[55] Agencia Española de Protección de Datos, "Drones y Protección de Datos", *Agencia Española de Protección de Datos*

[56] Agencia Española de Protección de Datos, "Drones y Protección de Datos", *Agencia Española de Protección de Datos*. Página 5.

de operaciones no es de aplicación el reglamento, pues no hay ninguna recopilación de datos.

Las operaciones con riesgo de tratamiento de datos personales de forma colateral se definen como operaciones en las que la finalidad no es la recopilación de información personal, pero puede que se produzca como un efecto colateral de la actividad principal[57]. Un ejemplo de este tipo de actividad puede ser, por ejemplo, una inspección topográfica de un terreno cualquiera. El fin no es el tratamiento de datos personales de ninguna persona, pero si una persona esta paseando por ese terreno en el momento del vuelo, el dron va a captar su imagen de forma colateral. Por tanto, en este ejemplo la actividad era la de inspección, pero de forma colateral ha recabado datos personales. La recolección colateral de los datos se puede producir porque sea inevitable recoger los datos en segundo plano en el desarrollo de la actividad, porque sea inevitable para la actividad o por las características concretas de la actividad, como en el caso de que el piloto no pueda mantener el contacto visual con el dron y tenga que volar a través de imágenes transmitidas por una videocámara[58].

En el caso de las operaciones en las que el tratamiento de datos es el fin último de la actividad, es de absoluta aplicación la LOPD. En el caso de que la actividad sea la de videovigilancia le es de aplicación las normas concretas sobre videovigilancia de la Ley. En el resto de las actividades, como puede ser, por ejemplo, la grabación de un spot publicitario es necesario, entre otras cosas, distinguir si el operador del dron va a ser el encargado del tratamiento de los datos de carácter personal. En el caso de que sea el tercero que ha contratado al operador el que utilizará los datos, es responsabilidad de este cumplir con la legislación. Si es el propio operador el que se encargará de procesar los datos recogidos por encargo, entonces es él el responsable[59].

Por tanto, en cada apartado se mencionarán las tres categorías. Con ello se quiere comprobar si esta guía recoge todos los principios fundamentales del uso de drones y la captación de datos.

---

[57] *Ibid*, página 6

[58] Agencia Española de Protección de Datos, "Drones y Protección de Datos", *Agencia Española de Protección de Datos*, página 6

[59] Agencia Española de Protección de Datos, "Drones y Protección de Datos", *Agencia Española de Protección de Datos*, página 8.

2.1.1. Uso legítimo y proporcionado

Desde el principio del debate sobre la legislación del uso de drones se estableció que el tratamiento de la información obtenida a través de ellos solo podía realizarse cuando *"se persiga un fin legítimo, explicito o por motivos justificados, necesario en un estado democrático y en la medida de tomada pueda considerarse proporcionada al propósito perseguido"*[60], como confirmaron diversas sentencias del Tribunal de Derechos Humanos[61]. Por tanto, la recopilación de datos tiene que ser legal y perseguir un fin legítimo. Esto se dará en el caso de que[62] (i) el interesado proporcionase consentimiento, (ii) en base a la ejecución de un contrato válido entre dos partes, como puede ser entre una empresa o particular y un operador de drones, (iii) para cumplir una obligación legal, (iv) para cumplir con un interés público, (v) para satisfacer intereses legítimos siempre que no se realicen intromisiones ilegitimas y (vi) para proteger intereses vitales para el operador u otra persona que se lo encargue.

Por tanto, y a grandes rasgos, se considera se que tiene un fin legitimo para tratar datos obtenidos por un dron en los casos en los que se establezca por ley una obligación y por intereses legítimos del operador o una tercera persona que tenga algún tipo de relación, contractual o no con él. No será un fin legítimo, el tratamiento de datos obtenidos sin consentimiento o vulnerando los derechos de otras personas. Por tanto, una imagen recabada del interior de un domicilio no es legítima, pues se ha obtenido en violación de un derecho fundamental del afectado. Es en este momento en el que la normativa sobre el derecho fundamental a la intimidad cobra importancia.

La legislación española sobre protección a la intimidad se contiene básicamente 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[63]. Es necesario hacer una distinción del derecho a la intimidad, por un lado, y el derecho a la propia imagen, por el otro. El primero persigue, en palabras del Tribunal Constitucional, *"proteger la esfera de lo privado y de*

---

[60] González Puente, C., González Botija, F., "Los drones y los derechos fundamentales en la UE", *Revista Universitaria Europea* Nº 29, pp. 143-162. Página 155.

[61] Sentencia del Tribunal de Derechos Humanos (Gran Sala) de 7 de febrero de 2012, demandas número 40660/08 y 60641/08, párrafo 95.

[62] González Puente, C., González Botija, F., "Los drones y los derechos fundamentales en la UE", *Revista Universitaria Europea* Nº 29, pp. 143-162. Página 156.

[63] 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, «BOE» núm. 115, de 14/05/1982.

lo intimo"[64], mientras que el segundo garantiza que las personas *"decidan si permiten la captación o difusión de su imagen por un tercero"*[65].

Es necesario recalcar que no todas las intromisiones a la vida privada son violaciones del derecho de intimidad. No es un derecho absoluto, y por tanto es necesario realizar un juicio de proporcionalidad y de ponderación para valorar el acto que se pretende realizar y el derecho que se va a restringir, teniendo en cuenta tanto la legislación, como las circunstancias en las que se realizará o realizó el acto y las costumbres de la sociedad. El Tribunal Supremo ha establecido con respecto a este juicio que es necesario valorar si la captación de las imágenes era el objetivo final del uso del dron o si es un efecto colateral o accesorio[66]. En el caso de que se grabe o se obtengan datos por parte de un dron del interior de un domicilio privado, sin consentimiento y aunque sea de forma colateral se reputará de forma general como una violación de la inviolabilidad del domicilio, como se estableció en la Sentencia del Tribunal Supremo 1709/2016. En esta sentencia, el Tribunal establece que *"la protección constitucional frente a la incursión en un domicilio debe de abarcar, ahora más que nunca, […] tanto frente la irrupción inconsentida del intruso en el escenario doméstico, como respecto de la observación clandestina de lo que acontece en su interior, si para ello es preciso valerse de un artilugio técnico de grabación o aproximación de las imágenes"*[67].

Por tanto, y a grandes rasgos, si se graba a una persona sin su consentimiento en su esfera de intimidad o en su domicilio, realizando actividades privadas o en lugares en los que se presupone una cierta intimidad, se estará produciendo una intromisión ilegitima de su derecho. Si, sin embargo, es con un fin absolutamente diferente y la captación es colateral o involuntaria y, en tal caso, se adoptan las medidas precisas de "anonimización" o de protección a los derechos personales o se obtiene el consentimiento de la persona, la intromisión es legitima, y por tanto, concorde con la protección de datos.

En resumen, se puede utilizar un dron y recabar datos con el siempre que se utilice con un fin legítimo, como puede ser el uso profesional o el ocio, mientras que las imágenes que se recojan no vulneren los derechos de otras personas.

---

[64] Sentencia del Tribunal Constitucional 197/1991, de 17 de octubre (ECLI:ES:TC:1991:197)

[65] Sentencia del Tribunal Constitucional 14/2003, de 28 de enero (ECLI:ES:TC:2003:14)

[66] Sentencia del Tribunal Supremo 1042/2007, de 22 de febrero (ECLI: ES:TS:2007:1042)

[67] Sentencia del Tribunal Supremo 1709/2016, de 20 de abril (ECLI: ES:TS:2016:1709)

En la "Guía sobre Drones y Protección de Datos" de la AEPD no se indica específicamente que es un uso legítimo del dron. Se comienza directamente realizando la diferenciación sobre los tipos de usos que se le puede dar. A pesar de ello, por esta clasificación se puede inferir que los usos que se le pueden dar al dron son los recreativos y los profesionales, que respeten en todo caso la protección de datos.

2.1.2. Minimización de los datos

En el uso de datos es necesario utilizar un principio de proporcionalidad en la recogida de los mismos. Por tanto, siempre que el uso del dron no pueda evitar la recogida de datos, situación generalizada para todos los drones, es necesario aplicar el principio de minimización de datos. Este principio, que se basa en adoptar todas las medidas posibles para minimizar los datos que se recogen, se tiene que aplicar desde el diseño hasta el tratamiento y el uso de ellos[68], como se establece en el artículo 25.1 del RGPD. En todo caso, hay que respetar los principios legales sobre la protección legal de los datos personales, contenido en el artículo 5 del RGPD.

Desde el diseño de un dron se pueden aplicar medidas que minimicen los datos, tanto por parte del fabricante como por el operador antes de iniciar el vuelo. Desde el punto de vista del diseño del dron, es necesario que los fabricantes sean conscientes de las capacidades de intromisión de los aparatos, y por tanto los diseñen para que la recogida de datos sea la menor posible. Las propuestas que se han realizado son principalmente dos[69]. Por un lado, se ha propuesto involucrar a los organismos encargados de la protección de datos de los lugares donde se fabriquen los aparatos como consultores y, por otro, el establecimiento de medidas predeterminadas por fábrica que establezcan software de privacidad por defecto (como establece el artículo 25 del RGPD). Una de las herramientas que se pueden utilizar, y en las que más han incidido las recomendaciones de la Comisión y de la AEPD, son las técnicas de anonimización[70], con las que se permite eliminar los datos protegidos por la ley directamente por el dron, de forma que los operadores ni

---

[68] i Marquès, M. C., "Drones recreativos y responsabilidad civil (Tras la reforma de 2017)"*, Revista de Derecho Civil,* vol. 6, nº 1, 2019, pp. 297-333. Página 327.

[69] González Puente, C., González Botija, F., "Los drones y los derechos fundamentales en la UE", *Revista Universitaria Europea* Nº 29, pp. 143-162. Página 157.

[70] Grupo de Trabajo sobre el Artículo 29 "Opinión 05/2014 sobre Técnicas de Anonimización", Comisión Europea, 2014

siquiera puedan obtener la información privada una vez descarguen los datos del dron[71]. Una de las técnicas más utilizadas es el software de análisis de vídeo anónimo, con el que se permite que el dron establezca de forma automática, desde el momento de la recopilación de datos, borrosidad u otros efectos gráficos sobre el rostro de las personas que ha grabado o directamente elimine los segmentos de los videos para impedir su identificación[72]. El avance de la tecnología es tal, que ya se han desarrollado software que permiten revertir la borrosidad de los rostros e identificar a la persona[73]. Pero esta tecnología, a pesar de ser peligrosa, no es accesible para la mayoría. Por tanto, las técnicas de anonimización continúan siendo las más seguras para proteger los datos.

El principio de minimización de los datos también tiene que ser respetado por los operadores durante los vuelos. Los operadores durante el vuelo solo tienen que recopilar los datos absolutamente necesarios para cumplir con el fin legítimo del vuelo. Para ello, deben de utilizar los sensores correctos y que menos intromisión provoquen[74]. Por ejemplo, si se quiere grabar un parque público para un anuncio, se tienen que utilizar cámaras fotográficas con la resolución justa para conseguir el objetivo, pero no cámaras multiespectrales, ni de detección de móviles o puntos de wifi. Pero el cumplimiento de esta obligación no se puede dejar al arbitrio de cada operador, sino que es necesario la creación de códigos de conducta por parte de los Estados[75] que permitan la identificación y la sanción de todo aquel que no lo cumpla. Del mismo modo, en los lugares en los que la regulación del uso de drones solo se permite en unas zonas concretas, es recomendable que las autoridades pertinentes que designen estos espacios publiquen mapas claros y públicos, para que tanto los operadores, como los particulares sepan que en esa zona concreta puede haber drones recopilando datos[76].

---

[71] Cavoukian, A., "Privacy and drones: Unmanned aerial vehicles", Ontario: Information and Privacy Commissioner of Ontario, Ontario, Canada, 2012. Página 18-19.

[72] Navas Navarro, S. "Derecho e inteligencia artificial desde el diseño. Aproximaciones", en Navas Navarro. S (Dir) *Inteligencia Artificial. Tecnología y Derecho*, Tirant lo Blanch, Valencia, 2017. Página 65.

[73] Cichowski J. y Czyzewski, A., "Reversible Video Stream Anonymization for Video Surveillance Systems Based on Pixels Relocation and Watermarking," *IEEE International Conference on Computer Vision Workshops*, 2011.

[74] i Marquès, M. C., "Drones recreativos y responsabilidad civil (Tras la reforma de 2017)", *Revista de Derecho Civil*, vol. 6, nº 1, 2019, pp. 297-333. Página 327.

[75] Para poder observar un ejemplo de un código de conducta, consultar el Código de Conducta de la Agencia Española de Protección, llamado "Drones y Protección de Datos", citado supra.

[76] Para poder observar un ejemplo de un código de conducta, consultar el Reglamento italiano sobre

En el caso de que el operador haya recogido datos personales durante el vuelo y que estos no hayan sido eliminados por el dron automáticamente, es obligatorio que la persona encargada del procesamiento de los datos los elimine con la mayor prontitud posible de forma permanente e irrecuperable (artículo 5.1.e RGPD).

En la Guía de la AEPD se habla extensamente de la minimización de datos. Es el foco fundamental de todas las recomendaciones. Para las operaciones que no incluyen un tratamiento de datos personales, en las que se incluye toda actividad recreativa, se indica que antes de compartir ninguno de los datos obtenidos por los drones, es necesario asegurarse de que no se puede identificar a ninguna persona. En el caso contrario, se tienen que anonimizar.

En las operaciones con riesgo de tratamiento de datos personales de forma colateral o inadvertida, se hace mucho hincapié en la responsabilidad del propio operador del dron, para que vuele, por ejemplo, en horas poco concurridas o que no capture datos durante todo el vuelo, sino que encienda los sensores en momentos puntuales de la operación. Igualmente hace referencia a la minimización de datos desde el diseño, y sugiere reducir la resolución de la cámara o la granulidad de la geolocalización.[77]

En las operaciones que tienen por finalidad el tratamiento de datos, la obligación de la minimización de datos recae al operador del dron. Por tanto, la persona que esta realizando el vuelo es el responsable de recoger la información justa y necesaria para cumplir con la función encargada. Por tanto, tiene que escoger la tecnología más adecuada para el fin, eliminar o anonimizar cualquier dato redundante, implementar ajustes desde el inicio que minimicen la captación y hacer que los drones sean visibles e identificables.[78]

2.1.3. Consentimiento del afectado

El consentimiento del titular es una de las circunstancias que convierten la recopilación de datos en algo legítimo. La obtención del consentimiento en el uso de drones es un asunto en el que hay mucha discusión doctrinal, principalmente por las propias características del dron. Se reconoce que no se tiene que apreciar de una forma concreta,

---

vehículos aéreos pilotados a distancia, concretamente el artículo 23.

[77] Agencia Española de Protección de Datos, "Drones y Protección de Datos", *Agencia Española de Protección de Datos*, página 7.

[78] *Ibid,* página 8.

sino tan solo demostrar que el afectado era consciente de que sus datos estaban siendo recabados y que accedió a ello (artículo 7 del RGPD). El consentimiento tiene que ser en todo caso específico, informado, inequívoco y libre (artículos 3.h y 6.1 de la LOPD), y que se haya obtenido como consecuencia de los deberes de información impuestos sobre el operador (artículo 11 de la LOPD). El Reglamento General de Protección de Datos en su artículo 13 y la LOPD en su artículo 13 establecen la obligación de comunicar una serie de datos, tales como la identidad del operador, los fines del tratamiento de datos y la existencia de sus derechos sobre protección de datos… siempre que ello sea posible. Es muy difícil que en grandes vuelos en los que se cubre mucho terreno o en el los que se va a sobrevolar un área en el que pasan muchas personas, recabar el consentimiento de todos ellos, en especial si, como suele ocurrir, son personas anónimas y desconocidas para el operador[79]. Existen multitud de proposiciones para cumplir con estos deberes.

En primer lugar, la Agencia Catalana de Protección de Datos propuso que la información a los afectados se realizara a través de la colocación de carteles por toda el área sobre la que el dron iba a sobrevolar[80], aplicando los mismos principios y exigencias que a los sistemas de videovigilancia[81]. Esta opción se ve respaldada parcialmente por numerosos expertos, que concuerdan en que esta es una medida adecuada para espacios cerrados o muy delimitados[82]. Si es un evento en un espacio cerrado, como puede ser durante un espectáculo deportivo o durante un mitin, en los que es fácil colocar carteles a la entrada de los eventos. Del mismo modo, se puede anunciar el uso de drones a través de megafonía o de las pantallas de televisión que suelen retransmitir estos eventos[83]. A pesar de ello, esta técnica tiene principalmente dos problemas de uso si se aplica a nivel general para cualquier operación. La primera de ellas es que, para el uso recreativo, esta medida es tremendamente gravosa. Es imposible para un operador privado asumir el coste de cada vez que quiere realizar un vuelo con su dron tener que imprimir carteles y colocarlos

[79] Grupo de Trabajo sobre el Artículo 29, "Informe 01/2015 sobre privacidad y protección de datos relacionados con la utilización de Drones", Comisión Europea, 2015.

[80] Agencia Catalana de Protección de Datos, "Cumplimiento del deber de información en el uso de `drones´(CNS 12/2014)", *Agencia Catalana de Protección de Datos,* 2014

[81] Instrucción 1/2009, de 10 de febrero, sobre el tratamiento de datos de carácter personal mediante cámaras con fines de videovigilancia, DOGC número 5322, de 19 de febrero, Agencia Catalana de Protección de Datos.

[82] Muñoz, T., "Los drones y la protección de datos de carácter personal", *DGE Bruxelles Consulting Group*

[83] González Puente, C., González Botija, F., "Los drones y los derechos fundamentales en la UE", *Revista Universitaria Europea* Nº 29, pp. 143-162. Página 159.

por toda la zona en la que va a grabar. La segunda es que estos carteles no se pueden reutilizar de un evento a otro, dado que la información que se exige que se facilite, conforme a lo antes señalado, no es igual para dos vuelos, a menos que sean vuelos que se produzcan siempre del mismo modo, como pueden ser los de videovigilancia. Esto añade aún más peso al volumen de obligaciones de los operadores, además de no corresponderse con las medidas contra el cambio climático que tienden a imponer todos los Estados.

La segunda propuesta es el uso de las nuevas tecnologías para comunicar que se operará un dron por una zona. Se ha propuesto la creación de recursos web y el uso de redes sociales para crear un lugar con toda la información a tiempo real de los vuelos que se están produciendo[84]. Esto permitiría que todas las personas que lo quisieran pudieran consultar la página web para saber si donde quieren ir hay operaciones de drones o no. Esta medida elimina los problemas que acarreaba la primera propuesta sobre el elevado costo para el uso recreativo y sobre la contaminación. El problema es que la seguridad que proporcionada los carteles también se disipa. Mientras que en la primera propuesta era altamente probable que cualquier persona que se encontrará en el área de grabación hubiese visto al menos uno de los carteles, no se puede asegurar que las personas consulten este recurso cada vez que salgan a la calle. No es lógico pensar que una persona que va a caminar por el campo o a correr por el parque va a comprobar antes de ir una página para ver si se van a producir vuelos de drones y para dar su consentimiento a que sea grabado.

La tercera propuesta, ya esbozada en el apartado de la minimización de datos, es la publicación por parte del Estado de mapas en los que se indique de forma clara todos los lugares en los que los drones pueden realizar sus vuelos[85]. El principal problema del que adolece está opción es la misma que en el caso anterior, en el sentido de que es difícil que se den a conocer estos mapas al público en general, para que sean consientes de que están siendo grabados.

---

[84] Grupo de Trabajo sobre Protección de Datos y Telecomunicaciones, "Working Paper on Privacy and Aerial Surveillance", Reunión 52, Berlín, Alemania, 2013.

[85] González Puente, C., González Botija, F., "Los drones y los derechos fundamentales en la UE", *Revista Universitaria Europea* Nº 29, pp. 143-162. Página 160.

En cuarto y último lugar se encuentra la propuesta realizada por el Ministerio de Medio Ambiente en Francia, por la cual cuando un dron sobrevuela un área con personas se consideraría suficiente que el operador informara en persona a los afectados y estuviera disponible para contestar a sus preguntas[86]. Esta última opción puede ser especialmente útil para los vuelos recreativos, ya que en principio se presuponen que van a cubrir poco espacio y se realizaría de forma esporádica. El problema que plantea es en vuelos en los que se va a cubrir una distancia mayor, de forma que es imposible hablar con todo el mundo que aparezca en las imágenes.

Estas propuestas, a pesar de que cada una tiene sus puntos fuertes, no tienen en cuenta el desarrollo actual de las nuevas tecnologías. Como se indicaba, los drones son capaces de detectar todos los dispositivos móviles que se encuentren alrededor de su zona de vuelo. Es un hecho que todas las personas, al salir de casa, llevan un teléfono móvil encima. También es cierto que la mayoría lleva la geolocalización y los datos activados, para el uso, por ejemplo, de aplicaciones de navegación. Una posible solución que permitiría que todas las personas de una zona conozcan de forma automática que un dron se encuentra operando en la zona es que se incluya en la configuración la opción se envíe de forma automática un mensaje a los teléfonos en el área de recogida, para alertarles de que se está llevado a cabo un vuelo. En este contexto, resulta fundamental para que no se produzca otra posible violación de la normativa de protección de datos que los datos utilizados para localizar el móvil y enviar el mensaje no sean guardados por el dron en cuestión, de forma que no los almacene en ningún momento o los destruya de forma automática.

La Guía de la AEPD no menciona prácticamente el consentimiento. Este hecho es, sin duda, sorprendente. La única referencia que se hace a este principio es en las operaciones que tienen por finalidad un tratamiento de datos personales. Se indica que se tienen que habilitar mecanismos de información que sean claros y transparentes, y se menciona como ejemplos señalizar, hojas informativas, publicaciones en redes sociales, periódicos, folletos, posters… En los que se indique los datos necesarios para identificar a la persona que va a tratar los datos y los derechos que tienen los afectados[87].

---

[86] Direction générale de l'Aviation civile "Usage d'un dron de loisir", *Ministere de L'Environnement, de L'Energie et de la Mer*, Francia

[87] Agencia Española de Protección de Datos, "Drones y Protección de Datos", *Agencia Española de*

2.1.4. Conservación de los datos

En lo que respecta a la conservación de datos hay dos obligaciones principales. La primera de ellas es la eliminación de todos los datos no esenciales, y la segunda la protección de estos contra cualquier destrucción o robo.

En lo que respecta a la eliminación, es de aplicación lo indicado en el principio de minimización de datos, es decir, la eliminación de todos los datos no esenciales para el fin perseguido por la operación de forma permanente. Esta eliminación permanente, además, tiene que ser irreversible, por lo que no se puede recuperar la información de ninguna forma[88]. Por tanto, se podrán conservar los originales de las imágenes que el dron ha obtenido tras eliminar cualquier información sensible.

Por otro lado, la protección de los datos se tiene que aplicar en todas las etapas del tratamiento y el procesamiento de los datos. En un primer lugar, es necesario proteger los datos en la transferencia entre el sensor a la plataforma en la que se vayan a procesar[89]. Esto es, es necesario proteger los sensores y las memorias donde almacenan la información, como tarjetas de memoria. Una opción para ello es la protección de los compartimentos donde se almacenan estos dispositivos desde el diseño, como por ejemplo poniendo un candado por código. En lo que se refiere ya al procesamiento de los datos, el Grupo de Trabajo sobre el artículo 29 esboza ciertas recomendaciones, que son (i) que a los datos acceda el menos número posible de personas, (ii) que se fragmenten los datos y dar acceso limitado a cada una de las personas autorizadas, (iii) que el almacenamiento sea encriptado y que se realicen las menores transferencias posibles, (iv) que se establezcan registros detallados sobre el acceso a los datos por parte de cada persona autorizada, (v) que los periodos de conservación de los datos sea lo menos prolongados posibles y (vi) que se garantice que cualquier violación de la normativa de protección de datos se va a notificar a las autoridades pertinentes[90]. Para poder cumplir con estas sugerencias, se recomienda la utilización de programas específicos creados para

---

Protección de Datos, página 8.

[88] i Marquès, M. C., "Drones recreativos y responsabilidad civil (Tras la reforma de 2017)", *Revista de Derecho Civil*, vol. 6, nº 1, 2019, pp. 297-333. Página 328.

[89] González Puente, C., González Botija, F., "Los drones y los derechos fundamentales en la UE", *Revista Universitaria Europea* Nº 29, pp. 143-162. Página 160.

[90] Grupo de Trabajo sobre el Artículo 29, "Informe 01/2015 sobre privacidad y protección de datos relacionados con la utilización de Drones", Comisión Europea, 2015.

registrar todos los movimientos y acciones que se realicen con los datos, así como la eliminación automática pasado un periodo de tiempo de forma permanente de todos los datos[91].

La conservación de datos respetando las recomendaciones emitidas por el Grupo de Trabajo citado solo son factibles para operadores profesionales, que tienen la necesidad y los medios para invertir dinero en este tipo de programas. Para el uso recreativo de los drones, lo más lógico es recomendar que los datos recogidos nos se puedan compartir por redes sociales, y que se eliminen cuando dejen de ser útiles.

Por último, es necesario también proteger los datos frente ataques exteriores, es decir, ataques de hackers (artículos 32 y siguientes del RGPD).

En la Guía de la AEPD tampoco se hace señala mucho las obligaciones de conservación de datos. En las operaciones con riesgo de tratamiento de datos personales de forma colateral o inadvertida tan solo se indica que se tiene que evitar el almacenamiento de información que contenga datos personales[92]. En el caso de operaciones que tienen por finalidad el tratamiento de datos personales, se realiza una recomendación mucho más acorde con lo señalado anteriormente, en la que se indica que se tienen que poner todas las medidas necesarias para asegurar los datos e impedir ningún tipo de filtración[93].

2.2. Excepciones y limitaciones a la aplicación de la normativa

Tanto la legislación europea como la española recogen excepciones a la aplicación de su marco normativo en determinados supuestos expresamente previstos de captación de datos por drones. En concreto, el Reglamento General de Protección de Datos en su artículo 2.2.c) y la LOPD en su artículo 2.2.a) excluyen de su aplicación la llamada "exención del hogar", por la cual los datos que una persona física particular recoge durante el uso recreativo de los drones no quedan sujetos a la normativa de protección de datos.

---

[91] González Puente, C., González Botija, F., "Los drones y los derechos fundamentales en la UE", *Revista Universitaria Europea* Nº 29, pp. 143-162. Página 161.

[92] Agencia Española de Protección de Datos, "Drones y Protección de Datos", *Agencia Española de Protección de Datos*, página 7.

[93] *Ibid*, página 8.

Esta "exención del hogar" que se da al uso recreativo de drones ha sido matizado por el Tribunal Superior de Justicia de la Unión Europea[94], que indica que solo se puede aplicar a los datos recogidos en actividades recreativas llevadas a cabo en la vida privada. A pesar de ello, el hecho de que una actividad se lleve a cabo de forma recreativa no significa que no haya que respetar los derechos del resto de las personas. Esto llevó al Tribunal a delimitar que en todos los casos de uso recreativo de drones en los que los datos (i) se difundiesen a un número indefinido de personas o muy amplio, (ii) no tuvieran que ver con una persona relacionada estrechamente con el operador del dron, (iii) se trataran con mucha frecuencia y volumen, indicando una actividad profesional, (iv) se hubiesen recogido de forma coordinada con otros individuos o (v) provocaran un grave perjuicio a la persona a la que pertenecen o supusieran una intromisión ilegitima en su derecho a la intimidad, los datos estaban sujetos a la normativa de protección de datos[95]. Además, toda obtención de imágenes por drones de videovigilancia, controlado por una persona física particular para vigilar su domicilio y que cubre un espacio público, como puede ser una acera, tampoco puede acogerse a la exención[96].

La limitación de esta exención era necesaria para evitar dejar al arbitrio de cada piloto aficionado la decisión de si se le aplicaba o no. Además, estas delimitaciones cobran especial importancia en el mundo interconectado en el que vivimos a día de hoy, en el que todos los contenidos se cuelgan en redes sociales. Por tanto, el simple hecho de subir a una red social los datos obtenidos por un dron, como imágenes o videos, ya entra dentro de una difusión amplia de los datos, desencadenando la protección inmediata de las leyes sobre protección de datos. La delimitación de la exención actúa como una garantía para todas aquellas personas que han sido grabadas por un dron y que no tienen porque querer que esos datos se encuentren en Internet.

Por otro lado, también es necesario mencionar que los principios mencionados anteriormente no operan siempre con la misma fuerza. Mientras que el uso legitimo de los drones, que protege el derecho a la intimidad de terceros, como la minimización de

---

[94] Sentencia del Tribunal Superior de Justicia de la Unión Europea (Sala Primera) de 6 de noviembre de 2003, asunto C-101/01, procedimiento penal entablado contra Bodil Lindqvust (ECLI:EU:C:2003:596)

[95] González Puente, C., González Botija, F., "Los drones y los derechos fundamentales en la UE", *Revista Universitaria Europea* Nº 29, pp. 143-162. Página 151.

[96] Sentencia del Tribunal Superior de Justicia (Sala Cuarta) de 11 de diciembre de 2014, asunto C-212/13, František Ryneš contra la Agencia checa de protección de datos de carácter personal (ECLI:EU:C:2014:2428).

datos siempre tienen que estar presentes, el consentimiento no es necesario bajo ciertas circunstancias, como estableció el Tribunal Superior de Justicia de la Unión Europea en el caso contra Google por Google Street View[97]. En este caso, Google, a través de drones, coches y bicicletas con cámara, grababa las calles de las ciudades y a las personas que se encontraban en ellas para subirla a su aplicación Google Maps. El Tribunal falló, como resume la Doctora en Derecho de la Universidad Autónoma de Barcelona Marina Castells i Marquès, que *"cuando el tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable y no prevalezcan los derechos y libertades fundamentales del interesado no es necesario que el afectado consienta. De modo que el tratamiento será lícito cuando se cumplan con los dos requisitos acumulativos mencionados, sin que puedan imponerse exigencias adicionales"*[98].

El derecho a la intimidad es un derecho fundamental, que en un juicio de ponderación prevalece en la mayoría de las ocasiones. Pero esto no hace que sea un derecho absoluto, que coarte la libertad del resto en el uso de drones. El equilibrio, que a mi parecer encuentra esta sentencia de forma muy acertada, se encuentra en la identificación del afectado. Si los datos recopilados en ningún caso pueden llevar a la efectiva identificación, entonces no es necesario que estos den su consentimiento.

Este razonamiento y esta sentencia facilita mucho el uso del dron. Por ejemplo, para un profesional que se dedica a la topografía y que tienen un trabajo que cubre varios kilómetros, es mucho más sencillo poder volar, respetando los principios de anonimizarían, sin tener que pedir permiso a todas las personas que se encuentren en el área de trabajo.

2.3. Guía de Recomendaciones de la Agencia de Protección de Datos

La Guía de la AEPD tiene una gran importancia. Es un hecho que los usuarios de drones, en especial los recreativos, no van a buscar la legislación sobre protección de datos en la ley. Es mucho más sencillo para ellos que la normativa venga recogida en una sola guía, de fácil comprensión y que sea accesible para todos.

---

[97] Sentencia del Tribunal Superior de Justicia de la Unión Europea (Sala Tercera) de 24 de noviembre de 2011, asuntos acumulados C-468//10 y C-469/ (ECLI:EU:C:2011:777).

[98] i Marquès, M. C., "Drones recreativos y responsabilidad civil (Tras la reforma de 2017)", *Revista de Derecho Civil*, vol. 6, nº 1, 2019, pp. 297-333. Página 327.

Para que una Guía pueda cumplir con su función de difusión de la normativa, no puede ser solo un compendio de normas. Al contrario, debe de ser comprensible. Esta norma cumple con este precepto, dado que explica las obligaciones en un lenguaje preciso y claro. A pesar de ello, es necesario analizar si las recomendaciones recogen todos los principios básicos mencionados anteriormente.

Creo que la Guía comete un fallo asimilando todos los vuelos de drones recreativos a actividades en las que no existe el riesgo de tratamiento de datos. Por tanto, lo que realiza es la asimilación de todos los vuelos a la exención del hogar explicada anteriormente. Como se ha dejado claro, esta exención de la normativa de protección de datos no es absoluta, y tiene muchas excepciones, entre las que se encuentra difundir un video en redes sociales o recoger datos de personas que no forman parte del circulo intimo del piloto. Debería dejarse mucho más claro en la Guía que si se recogen datos de cualquier persona se tiene que respetar la normativa igual.

En lo que se refiere a si la Guía refleja los principios básicos de la normativa de protección de datos, en primer lugar, no menciona los usos ilegítimos del dron. En especial, tendría que mencionar qué datos son ilegales de obtener. Como ya se ha señalado, la normativa de protección de datos y el derecho a la intimidad está muy ligados entre ellos. Por tanto, es fundamental señalar que cualquier imagen recogida en vulneración de este derecho es también una violación de la normativa de protección de datos. Esto no se menciona en ningún apartado. Al contrario, el principio de minimización de datos queda explicado de forma detallada y clara para todas las operaciones.

Referente al consentimiento, da por hecho lo señalado en la sentencia del caso de Google Maps, pero en ningún momento lo explica. Cabe de todas formas resaltar que en lo que respecta a las operaciones cuyo fin es el tratamiento de datos, sugiere diferentes formas de obtener consentimiento, lo que aclara la problemática ya expuesta.

Por último, en lo que respecta a la conservación de datos, hace referencia a ello fundamentalmente en las operaciones cuyo fin es recoger datos. Creo que sería necesario extender la recomendación de destruir los datos no necesarios a todos los usos.

En resumen, esta Guía recoge de forma muy sintética los principios explicados anteriormente. Esta explicación no es muy detallada. Esto puede provocar que los operadores actúen con menos cuidado del necesario y no conozcan en profundidad todas las obligaciones que tienen que respetar. Es por ello por lo que sería recomendable una

reformulación de la Guía, en la que quede más claro que los principios mínimos son de exigencia para todos los pilotos de drones, sea cual sea el uso al que están destinados, para pasar a realizar recomendaciones más detalladas dependiendo de las circunstancias.

Podría ser muy recomendable que la Agencia de Protección de Datos y la Agencia de Seguridad Aérea impulsaran una iniciativa para que los fabricantes incluyeran esta Guía junto con las instrucciones de uso y por donde se puede volar. Esta medida permitiría una difusión mucho mayor de las normas, y evitaría el desconocimiento que alegan especialmente los aficionados al uso de drones.

Como ha quedado claro, la gran variedad de sensores disponibles para el uso de drones hace que los datos personales que puede recoger este aparato sean muchos. Es necesario tener una legislación, y sobre todo, instrumentos para difundirla de forma clara, que sea eficaz. La vulneración de el derecho a la intimidad y a la protección de datos puede acarrear consecuencias muy serias, como el robo de datos personales o la divulgación de secretos de una persona anónima. Como ya se ha dicho anteriormente, las personas solo somos verdaderamente libres en la intimidad, y por tanto, es fundamental crear el sentimiento de que pase lo que pase, las personas van a estar seguras y van a poder disfrutar de su vida privada.

V. DERECHO COMPARADO NORTEAMERICANO

Estados Unidos es uno de los países con más presencia de drones en el mundo[99] y no está afectado por los principios anteriormente enunciados establecidos por la legislación europea. Esto hace que sea una legislación diferente y que su análisis resulte de interés.

1. USO DE DRONES

El uso de drones en Estados Unidos esta regulado por dos leyes diferentes, dependiendo del uso y del peso del dron.

1.1. Uso comercial

Los drones de uso comercial, que pesen menos de 25 kg se regulan por el título 14 del *Code of Federal Regulations part 107*[100], que fue introducida por la *FAA Modernization*

[99] i Marquès, M. C., "Drones recreativos y responsabilidad civil (Tras la reforma de 2017)", *Revista de Derecho Civil*, vol. 6, nº 1, 2019, pp. 297-333. Página 326.

[100] Título 14, Sección 107, Code of Federeal Regulations, 2020.

and Reform Act of 2012[101]. La autoridad encargada de hacer cumplir con los preceptos recogidos en este título es la *Federal Aviation Administration* (*FAA*).

Las normas de uso de drones comerciales se pueden dividir en varias secciones de obligaciones. La primera de ellas son los requisitos que se exigen que cumplan los pilotos para poder hacer uso del dron[102]. Los primeros pasos para poder obtener la licencia de vuelo son tener más de 16 años y no haber sido vetados por la *Transportation Security Administration* (TSA). Una vez que han sido aprobados, se les exige que tengan conocimientos sobre aeronáutica básica, así como conocimientos de vuelo. Para demostrarlo, hay dos opciones. La primera de ellas es realizar un examen de conocimientos. La segunda es poseer una licencia de piloto de vuelos y haber pasado un examen de vuelo en los 24 meses anteriores a la solicitud del certificado. Una vez que se obtiene el certificado dura 2 años, tras lo cual es necesario renovarlo[103]. El sistema español, por otro lado, añade un paso más a todo este proceso, por lo que además de los conocimientos de vuelo se necesita una autorización por parte de la Agencia Estatal de Seguridad Aérea.

En lo que respecta a los requerimientos del propio dron, tiene que pesar menos de 25 kg y ser sometido a un examen para comprobar sus condiciones antes del comienzo de cada vuelo. Si este examen no se realiza, las multas por accidentes se aumentarán por imprudencia[104]. Solo pueden volar por el espacio denominado como G[105] Este régimen es muy similar al español, con la diferencia de que en España no existe la restricción de 25 kg.

Por último, es necesario mencionar las normas durante el vuelo de los drones[106]. La más importante y sobre la que pivotan todo el resto es, sin duda, la obligación de que el dron

---

[101] FAA Modernization and Reform Act of 2012, promulgada por el Senado y la Casa de los Representantes en el Congreso, Public Law N0112-95, 126 Stat 11.

[102] Federal Aviation Administration, "Summary of Small Unmanned Aircraft Rule (Part 107)", *Federal Aviation Administration News*, 21 de junio de 2016

[103] Federal Aviation Administration, "Summary of Small Unmanned Aircraft Rule (Part 107)", *Federal Aviation Administration News*, 21 de junio de 2016.

[104] Butler, D., "Drones and invasions of privacy: An international comparison of legal responses", *UNSWLJ*, vol. 42, 2019 pp. 1039-174. Página 1064

[105] Es el espacio aéreo más bajo, en el que no sobrevuelan los aviones.

[106] Federal Aviation Administration, "Summary of Small Unmanned Aircraft Rule (Part 107)", *Federal Aviation Administration News*, 21 de junio de 2016.

siempre se mantenga a la vista del operador. Esto significa que los operadores siempre deben tener contacto visual con el dron durante un vuelo, y no pueden volar a ciegas orientados por una cámara. Además, solo pueden volar como máximo a 120 metros de altura y con una velocidad de 86 nudos (unos 160 kilómetros por hora). Por último, no se puede volar sobre personas, desde un vehículo en marcha o cerca de aeropuertos. Para poder volar en circunstancias diferentes, se puede solicitar autorización a las autoridades competentes. Estas autorizaciones especiales para operaciones se conceden igual en España.

Todos los drones tienen que estar registrados en la *FAA* sin excepción, proporcionando el número de serie del dron, el nombre del operador, el seguro que lo cubre, y otros datos para facilitar la identificación en el cualquier caso, como en España.

La normativa de uso profesional es muy similar a la española, tanto en las circunstancias en las que se puede volar, los requerimientos de los drones y en la necesidad de pedir autorización para ampliar el rango de acción. Las principales diferencias se encuentran en cómo se obtiene la autorización de piloto de drones. El método estadounidense mantiene los requisitos necesarios para asegurar los conocimientos de los pilotos y la seguridad, incluso ampliándolos, al exigir que todos los pilotos hayan superado el proceso de la TSA. Pero el procedimiento es mucho más corto, ya que se realiza en una misma instancia, lo que ahorra tiempo y dinero. Esto lo consiguen principalmente designando a una misma entidad para que realice los test y conceda las autorizaciones de vuelo.

1.2. Uso recreativo

El uso recreativo de los drones se regula de forma separada por la *FAA Reauthorization Acto f 2018*[107]. Al igual que en el caso de los drones comerciales, tiene que pesar menos de 25 Kg para que se considere un dron de uso civil. Las principales diferencias se pueden encontrar en las otras categorías de regulación[108]. En lo que respecta a los conocimientos de los operadores, no se requiere que realicen ninguna prueba o que reciban la aprobación de ningún organismo. Del mismo modo, tienen que volar al menos a 5 millas (unos 8 kilómetros) de los aeropuertos, que no intercepten o molesten a aeronaves pilotadas, que

[107] FAA Reauthorization Act of 2018 (Division B of House Amendment to Senate Amendment to H.R. 305), Public Law Nº 115-254

[108] Winkler, S., Zeadally, S., y Evans, K. "Privacy and civilian drone use: the need for further regulation", *IEEE Security & Privacy*, vol. 16, nº5, 2018, pp. 72-80. Página 75.

siempre se mantengan a la vista del piloto. Tampoco pueden volar sobre personas. Por último, se permite el vuelo nocturno siempre que el dron esté equipado con luces que permitan determinar su posición a siempre a la vista en cualquier momento.

Como en el caso de los drones de uso comercial, cualquier dron de uso recreativo tiene que estar inscrito en el registro de la FAA[109]. Se está comenzando a gestar una modificación de la legislación que conllevaría que, como requisito indispensable para poder inscribir el dron, los operadores tengan que pasar un test online de conocimientos de vuelo y aeronáuticos básicos[110]. Esta modificación sería muy beneficiosa para la seguridad. Al igual que en España, es curiosos como mientras que en el uso profesional de los drones sea fundamental probar los conocimientos básicos, en el uso recreativo no.

El principal punto de diferencia entre España y Estados Unidos es que en este último país el uso recreativo de los drones sí que está regulado completamente por una ley. Sería recomendable que en España se regulara igualmente, para evitar la inseguridad jurídica y la posible libre interpretación de los aficionados.

2. PRIVACIDAD Y PROTECCIÓN DE DATOS

2.1. Captación de imágenes y derecho a la privacidad

En Estados Unidos, la Cuarta Enmienda[111] protege a los ciudadanos contra cualquier registro o incautación realizada de forma arbitraria por las autoridades del Estado. Este derecho a lo largo de los años y gracias a casos históricos del Tribunal Supremo de Estados Unidos tales como *Katz v. United States*[112] se ha extendido hasta cubrir el derecho a la privacidad. El Tribunal Supremo a establecido dos cuestiones que se deben de analizar en cualquier caso de violación de la privacidad, que son (i) si la persona a demostrado una expectativa de privacidad razonable, y si (ii) la sociedad reconoce esa expectativa razonable[113].

---

[109] *Id.*

[110] Federal Aviation Administration "Recreational Flyers & Modeler Community-Based Organizations: Changes Coming in the Future", *Federal Aviation Administration*.

[111] Fourth Amendment to the United States Constitution, Bill of Rights, 1971.

[112] Tribunal Supremo de Esatdos Unidos, 389 US 347, 361 (Harlan J) Katz v United States, 1967.

[113] Dwyer-Moss, J., "The Sky Police: Drones and the Fourth Amendment" *Albany Law Review*, vol. 81 ,nº 3, 2018, pp. 1047- 1070. Página 1058.

A pesar de que este Tribunal aún no ha establecido jurisprudencia sobre este caso, queda claro que el mismo examen se puede utilizar para el uso de drones. De esta forma, no se podrán grabar imágenes de personas siempre que estas se encuentren en lugares en los que se espera una expectativa de privacidad, como, por ejemplo, dentro de sus casas o apartamentos[114]. Por el contrario, en un jardín de una casa que no se encuentre vallado, o en el que la valla es lo suficientemente baja como para que una persona normal pueda observar a la perfección lo que ocurre en el interior, sí que se puede grabar, dado que en esos lugares no se tiene la expectativa de privacidad[115].

Toda violación de esta expectativa de privacidad se podrá llevar ante un tribunal bajo una *intrusion tort.* En línea con lo que es el sistema anglosajón, y dado que no ha llegado aún al Tribunal Supremo, cada juez aplica a cada caso el análisis indicado anteriormente, obteniendo resultados muy diferentes. Aún no hay una jurisprudencia consolidada sobre el asunto.

2.2. La protección de datos

En Estados Unidos, la Protección de Datos es un ámbito legislativo tremendamente segmentado, con normas muy desiguales entre los Estados. A nivel nacional, no existe ninguna norma de protección de datos federal, que se aplique a todos. A pesar de ello, la *National Telecommunications and Information Administration* (*NTIA*) creó en 2016 la *Voluntary Best Practices for UAS Privacy, Transparency and Accountability*[116], un manual de Buenas Prácticas sobre Protección de Datos. En él se hace una recopilación de las normas básicas que cualquier usuario de dron debe de tener en cuenta al recopilar datos en cualquier parte del país. Por tanto, indican las normas básicas que se deben de respetar en bajo cualquier jurisdicción de cualquier Estado[117].

Este manual divide las recomendaciones en tres bloques, las realizadas para drones de uso comercial, las de uso recreativo y los usados por la prensa.

---

[114] Butler, D., "Drones and invasions of privacy: An international comparison of legal responses", *UNSWLJ*, vol. 42, 2019 pp. 1039-174. Página 1064

[115] *Ibid,* página 1065.

[116] "Voluntary Best Practices for UAS Privacy, Transparency, and Accountability" *National Telecommunications and Information Administration*, 2016

[117] Winkler, S., Zeadally, S., y Evans, K. "Privacy and civilian drone use: the need for further regulation", *IEEE Security & Privacy*, vol. 16, nº5, 2018, pp. 72-80. Página 75.

En el primer bloque se habla de las recomendaciones para los drones de uso comercial, y se divide en los bloques de transparencia y consentimiento, datos recogidos, y procesamiento y conservación. El primero de los bloques se ocupa de la transparencia y el consentimiento que cualquier operador de uso comercial tiene que recabar si recoge datos privados de las personas[118]. Al igual que en la legislación española y europea, el consentimiento no tiene que ser explicito, sino que debido a las propias características del dron se permite el consentimiento implícito. Por otro lado, en este caso si que se recomienda un método para informar de las operaciones y recabar el consentimiento. Este método consiste en la publicación de una política de privacidad detallada en la página web corporativa. Esta recomendación no está exenta de polémica, ya que debido a cómo está redactado el texto deja mucho espacio a la interpretación personal que realicen los operadores. Es verdad que, al igual que la propuesta de creación de una página web en España, la publicación online permite un acceso sencillo. A pesar de ello, el problema continúa siendo el mismo, que es la baja probabilidad de que las personas consulten estas páginas antes de salir de casa[119]. Este problema se ve agravado en este caso, dado que la información ni siquiera se encuentra recogida en un solo lugar, esta diseminada, lo que hace que sea incluso más difícil localizarla. La parte positiva de esta política es que, en los casos en los que es imposible avisar a la persona concreta de que sus datos han sido recabados, ya sea porque ha sido un efecto colateral o indeseado, tener unas políticas de privacidad publicadas y accesibles para todo el mundo es una garantía contra los abusos[120].

El segundo bloque de recomendaciones se ocupa de la recopilación de los datos. Se define que los datos protegido son todos aquellos que puedan llevar a una identificación efectiva de la persona. La definición utilizada es muy similar a la española, al igual que el principio que se recomienda, el principio de la minimización de datos, utilizando herramientas como los softwares de anonimización de datos. La diferencia principal es que, en Estados

---

[118] "Voluntary Best Practices for UAS Privacy, Transparency, and Accountability" *National Telecommunications and Information Administration*, 2016. Página 5.

[119] Malaga, R. "Do Web Privacy policies Still Matter?" *Academy of Information & Management Sciences Journal,* vol. 17, nº 1, 2014, pp. 95-99. Página 99.

[120] Winkler, S., Zeadally, S., y Evans, K. "Privacy and civilian drone use: the need for further regulation", *IEEE Security & Privacy*, vol. 16, nº5, 2018, pp. 72-80. Página 76.

Unidos, debido a la falta de una legislación clara, se deja mucho más al arbitrio personal que conlleva la identificación efectiva de la persona. Se puede dar el caso de que una persona considere que por la publicación de un video en redes sociales en las que aparece de lejos la casa de una persona no pueden llevar a una identificación efectiva El problema es que, como en el caso de las técnicas de anonimización, la tecnología se ha desarrollado lo suficiente como para crear, por ejemplo, software de reconocimiento facial muy potentes, lo que provoca que se pueda reconocer a cualquier persona que no tenga la cara tapada[121].

El último bloque trata sobre el tratamiento y la conservación de los datos recopilados. En este caso, las recomendaciones son muy parecidas a las obligaciones en España y Europa. Los drones no pueden recopilar datos sin consentimiento o sin un fin legítimo o razón de peso, como la denomina la guía, no pueden mantenerlos más tiempo del absolutamente necesario y tienen que seguir las políticas de privacidad en su web. No hay ninguna indicación sobre el número de personas que pueden acceder a los datos, lo cual puede generar filtraciones de seguridad. La otra gran diferencia es que la Guía de la NTIA indica que está prohibido el uso de los datos para determinar aspectos laborables, de seguros de salud o sobre aspectos financieros[122].

En lo que se refiere a las recomendaciones para uso recreativo de los drones, la Guía de la NTIA es mucho más genérica, indicando las mismas normas que para los drones de uso comercial pero simplificadas[123]. Por ejemplo, se indica que se tiene que evitar grabar datos innecesarios o sin consentimiento y que se tiene que evitar en la medida de lo posible pasar sobre propiedad privada "siempre que no se tenga una buena razón". Además, se indica que se debe de almacenar la información en un lugar seguro.

Por último, hay un apartado separado para el uso de drones por parte de la prensa. En este caso se da mucha más libertad a este tipo de operadores bajo la primera enmienda y la libertad de expresión[124].

---

[121] *Ibid,* página 77.

[122] La guía, en su página 6 apartado 3(a) indica textualemtne: "*employment eligibility, promotion, or retention; credit eligibility; or health care treatment eligibility other than when expressly permitted by and subject to the requirements of a sector-specific regulatory framework."*

[123] "Voluntary Best Practices for UAS Privacy, Transparency, and Accountability" *National Telecommunications and Information Administration*, 2016 Página 8.

[124] *Ibid*, página 7.

La primera diferencia clara con el tratamiento aplicable en España es que en Estados Unidos se realiza una diferenciación entre los diferentes usos de los drones, mientras que en España todos los usos se ven obligados a cumplir con los mismos principios.

En el primer bloque, relativo al uso profesional, la regulación Española es mucho más detallada, y cubre muchas más eventualidades, protegiendo así mejor a los ciudadanos. A pesar de ello, se pueden ver que los principios se encuentran en ambos. En lo que se refiere al consentimiento, en España se busca un conocimiento más efectivo que el que se otorga por parte de una política de privacidad. En la recopilación de datos se aplica el principio de la minimización de datos. En el procesamiento y la conservación se busca igualmente que losa datos estén protegidos y que se eliminen lo antes posible.

En el uso recreativo de drones, las recomendaciones de la Guía de la NTIA son claramente insuficientes. Las recomendaciones que recoge son un punto medio, entre permitir que los drones de uso recreativo vuelen sin ninguna regulación y la regulación española. En la Guía de la NTIA no se hace referencia explicita sobre compartir los datos en internet, lo cual puede generar un grave problema de protección de datos. La protección de la intimidad y de la privacidad tiene que ser igual para cualquier persona.

VI. CONCLUSIÓN Y RECOMENDACIONES

Se han generado más datos en el último lustro que en toda la historia de la humanidad[125]. Por ello, la importancia de la protección de esos datos es fundamental. En un contexto en el que el uso de los drones ha crecido, es de gran importancia que exista una regulación concreta y clara para que se eviten abusos.

En España existe una regulación de uso de drones profesional muy detallada, que cubre cualquier situación. Esta norma debe de ser más comprensiva con la situación actual de las personas y, a ser posible, unificar el procedimiento de certificación, al estilo de Estados Unidos. No sucede lo mismo con el uso recreativo. Por tanto, es fundamental el desarrollo de una ley completa para proporcionar seguridad jurídica, en la que se incluya la obligación de pasar un test básico de conocimiento para poder registrar pilotar el dron.

[125] Cerveras Navas, L. "La primera en el peligro de la privacidad: La Unión Europea y la defensa del derecho fundamental a la protección de datos personales." *Boletín de la Academia Malagueña de Ciencias*, vol. 20, 2018, pp 9-17. Página 13.

En lo que se refiere a la protección de datos, los principios generales que se aplican a la mayoría de los vuelos de drones, sean recreativos o profesionales, son muy efectivos. A pesar de ello, es necesario adaptarlos al avance tecnológico. La única posibilidad es invertir para poder continuar asegurando la privacidad. Una investigación propuesta en este trabajo es el desarrollo de un programa que permita que se avise a todos los móviles del área de vuelo de que un dron esta en una operación.

Además, es necesaria la actualización y desarrollo de la Guía de Drones y Protección de Datos publicada por la Agencia Española de Protección de Datos, y completar su contenido para que refleje de forma más clara y comprensiva las obligaciones de los operadores de drones y los principios y límites aplicables para que no puedan llevar a error. La inclusión de esta Guía en los paquetes de todos los drones que se compren sería adicionalmente una forma de difundir estas normas y facilitar su cumplimiento.

Los drones han llegado para quedarse en la sociedad, por lo que el desarrollo de una normativa concreta va en beneficio de todos.

BIBLIOGRAFÍA

1. LEGISLACIÓN

Carta de los Derechos Fundamentales de la Unión Europea, DOUE núm. 83, de 30 de marzo de 2010, páginas 389 a 403.

Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

FAA Modernization and Reform Act of 2012, promulgada por el Senado y la Casa de los Representantes en el Congreso, Public Law Nº 112-95, 126 Stat 11.

FAA Reauthorization Act of 2018 (Division B of House Amendment to Senate Amendment to H.R. 305), Public Law Nº 115-254

Federal Aviation Administration "Recreational Flyers & Modeler Community-Based Organizations: Changes Coming in the Future", *Federal Aviation Administration* (disponible en https://www.faa.gov/uas/recreational_fliers/)

Fourth Amendment to the United States Constitution, Bill of Rights, 1971.

Instrucción 1/2009, de 10 de febrero, sobre el tratamiento de datos de carácter personal mediante cámaras con fines de videovigilancia, DOGC número 5322, de 19 de febrero, Agencia Catalana de Protección de Datos.

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

Ley 21/2003, de 7 de julio, de Seguridad Aérea, BOE núm. 162.

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, «BOE» núm. 115, de 14/05/1982.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, «BOE» núm. 294, de 6 de diciembre de 2018, páginas 119788 a 119857.

Orden ETU/1033/2017, de 25 de octubre, por la que se aprueba el cuadro nacional de atribución de frecuencias, BOE núm. 259, de 27 de octubre de 2017, páginas 103115 a 103478.

Real Decreto 1036/2017, de 15 de diciembre, por el que se regula la utilización civil de las aeronaves pilotadas por control remoto, y se modifican el 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 el Real Decreto 57/2002, de 18 de enero, por el que se aprueba el Reglamento de Circulación Aérea. BOE número 216, de 29 de diciembre de 2017

Real Decreto 57/2002, de 18 de enero, por el que se aprueba el Reglamento de Circulación Aérea, BOE núm. 17, páginas 2449 a 2450.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, Diario Oficial de la Unión Europea

Reglamento (UE) número 923/2012 de la Comisión, de 26 de septiembre de 2012, por el que se establecen el Reglamento del aire y disposiciones operativas comunes para los servicios y procedimientos de navegación aérea

Título 14, Sección 107, Code of Federeal Regulations, 2020.

2. JURISPRUDENCIA

Sentencia del Tribunal Constitucional 14/2003, de 28 de enero (ECLI:ES:TC:2003:14)

Sentencia del Tribunal Constitucional 197/1991, de 17 de octubre (ECLI:ES:TC:1991:197)

Sentencia del Tribunal de Derechos Humanos (Gran Sala) de 7 de febrero de 2012, demandas número 40660/08 y 60641/08.

Sentencia del Tribunal de Justicia de la Unión Europea (Sala Segunda) de 14 de febrero de 2019, asunto C-345/17, Sergejs Buivids con la intervención de la Agencia Estatal de Protección de Datos de Letonia (ECLI:EU:C:2019:122).

Sentencia del Tribunal Superior de Justicia (Sala Cuarta) de 11 de diciembre de 2014, asunto C-212/13, František Ryneš contra la Agencia checa de protección de datos de carácter personal (ECLI:EU:C:2014:2428).

Sentencia del Tribunal Superior de Justicia de la Unión Europea (Sala Primera) de 6 de noviembre de 2003, asunto C-101/01, procedimiento penal entablado contra Bodil Lindqvust (ECLI:EU:C:2003:596)

Sentencia del Tribunal Superior de Justicia de la Unión Europea (Sala Tercera) de 24 de noviembre de 2011, asuntos acumulados C-468//10 y C-469/ (ECLI:EU:C:2011:777).

Sentencia del Tribunal Supremo 1042/2007, de 22 de febrero (ECLI: ES:TS:2007:1042)

Sentencia del Tribunal Supremo 1709/2016, de 20 de abril (ECLI: ES:TS:2016:1709)

Tribunal Supremo de Esatdos Unidos, 389 US 347, 361 (Harlan J) Katz v United States, 1967.

3. DOCTRINA

"¿Qué podemos hacer con un dron?", *Agencia Estatal de Seguridad Aérea*, disponible en: https://www.seguridadaerea.gob.es/media/4629699/que_podemos_hacer_con_un_dron.pdf; última consulta 08/04/2020)

"Todas las partes de los drones explicadas al detalle", *Esenziale* (disponible en: https://esenziale.com/tecnologia/partes-drone/#Sensores; última consulta 08/04/2020)

"Voluntary Best Practices for UAS Privacy, Transparency, and Accountability" *National Telecommunications and Information Administration*, 2016 (disponible en https://www.ntia.doc.gov/files/ntia/publications/uas_privacy_best_practices_6-21-16.pdf; última consulta 08/04/2020)

Agencia Catalana de Protección de Datos, "Cumplimiento del deber de información en el uso de `drones´(CNS 12/2014)", *Agencia Catalana de Protección de Datos,* 2014 (disponible en: https://apdcat.gencat.cat/es/documentacio/resolucions-dictamens-i-informes/cercador/cercador-detall/CNS-12-2014-00001; última consulta 08/04/2020)

Agencia Española de Protección de Datos, "Drones y Protección de Datos", *Agencia Española de Protección de Datos* (disponible en https://www.aepd.es/sites/default/files/2019-09/guia-drones.pdf; última consulta 08/04/2020)

Aguilera, A. T., "La protección de datos en la Unión Europea: divergencias normativas y anhelos unificadores", Edisofer, Madrid, 2002.

Butler, D., "Drones and invasions of privacy: An international comparison of legal responses", *UNSWLJ*, vol. 42, 2019 pp. 1039-174.

Cavoukian, A., "Privacy and drones: Unmanned aerial vehicles", Ontario: Information and Privacy Commissioner of Ontario, Ontario, Canada, 2012.

Cerveras Navas, L. "La primera en el peligro de la privacidad: La Unión Europea y la defensa del derecho fundamental a la protección de datos personales." Boletín de la Academia Malagueña de Ciencias, vol. 20, 2018, pp 9-17.

Cichowski J. y Czyzewski, A., "Reversible Video Stream Anonymization for Video Surveillance Systems Based on Pixels Relocation and Watermarking," *IEEE International Conference on Computer Vision Workshops*, 2011.

De la Cal, L., "Tecnología china contra el coronavirus: de drones termómetro a apps que se chivan si te pones malo" *El Mundo*, 13 de marzo de 2020 (disponible en: https://www.elmundo.es/tecnologia/2020/03/13/5e68a08121efa08f5b8b475c.html;

última consulta 08/04/2020).

Delgado, V., "Historia de los drones", *El Dron* (disponible en: http://eldrone.es/historia-de-los-drones/; última consulta 08/04/2020)

Díaz Rojo, J.A., "Privacidad: ¿neologismo o barbarismo?", *Consejo Superior de Investigaciones Cientificas* (disponible en: http://webs.ucm.es/info/especulo/numero21/privaci.html; última consulta 08/04/2020)

Direction générale de l'Aviation civile "Usage d'un dron de loisir", *Ministere de L'Environnement, de L'Energie et de la Mer*, Francia (disponible en: https://www.ecologiquesolidaire.gouv.fr/sites/default/files/regles_usage_drone_loisir.pdf; última consulta el 08/04/2020)

Dwyer-Moss, J., "The Sky Police: Drones and the Fourth Amendment" *Albany Law Review*, vol. 81 ,nº 3, 2018, pp. 1047- 1070.

Federal Aviation Administration "Recreational Flyers & Modeler Community-Based Organizations: Changes Coming in the Future", *Federal Aviation Administration* (disponible en https://www.faa.gov/uas/recreational_fliers/; última consulta 08/04/2020)

Federal Aviation Administration, "Summary of Small Unmanned Aircraft Rule (Part 107)", *Federal Aviation Administration News*, 21 de junio de 2016 (disponible en https://www.faa.gov/uas/media/Part_107_Summary.pdf; última consulta 08/04/2020)

Finn R.L., Wright, D., Donovan, D., Jaques, L. y De Hert, P., "Privacy data protection and ethical risk in civilian RPAS operations. Final Report", Publications Office of the European Union,, Luxemburgo, 2014.

González Porras, A. J. "Privacidad en internet: los derechos fundamentales de privacidad e intimidad en internet y su regulación jurídica. La vigilancia masiva" Tesis, Universidad de Castilla La Mancha, 2015 (disponible en: https://ruidera.uclm.es/xmlui/bitstream/handle/10578/10092/TESIS%20Gonz%c3%a1lez%20Porras.pdf?sequence=1&isAllowed=y; última consulta 08/04/2020)

González Puente, C., González Botija, F., "Los drones y los derechos

fundamentales en la UE", *Revista Universitaria Europea* Nº 29, pp. 143-162.

Grupo de Trabajo sobre el Artículo 29 "Opinión 05/2014 sobre Técnicas de Anonimización", Comisión Europea, 2014

Grupo de Trabajo sobre el Artículo 29, "Informe 01/2015 sobre privacidad y protección de datos relacionados con la utilización de Drones", Comisión Europea, 2015.

Grupo de Trabajo sobre Protección de Datos y Telecomunicaciones, "Working Paper on Privacy and Aerial Surveillance", Reunión 52, Berlín, Alemania, 2013.

i Marquès, M. C., "Drones recreativos y responsabilidad civil (Tras la reforma de 2017)", *Revista de Derecho Civil*, vol. 6, nº 1, 2019, pp. 297-333.

Kharuf-Gutierrez, S., Hernández-Santana, L., Orozco-Morales, R., Aday Díaz, O., y Delgado Mora, I., "Análisis de imágenes multiespectrales adquiridas con vehículos aéreos no tripulados", *Ingeniería Electrónica, Automática y Comunicaciones*, vol. 39, nº 2.

Kharuf-Gutierrez, S., Hernández-Santana, L., Orozco-Morales, R., Díaz, A., y Kent Jr, M. B., "Pavesich, Property and Privacy: The Common Origins of Property Rights and Privacy Rights in Georgia", *J. Marshall LJ*, vol. *2*, nº 1, 2009.

Malaga, R. "Do Web Privacy policies Still Matter?" *Academy of Information & Management Sciences Journal,* vol. 17, nº 1, 2014, pp. 95-99.

McIntyre, T.C., "The elements of Torts", Callaghan and Company, 1895.

Muñoz, T., "Los drones y la protección de datos de carácter personal", *DGE Bruxelles Consulting Group* (disponible en: http://www.dge.es/home/quienes-somos/548-los-drones-y-la-proteccion-de-datos-de-caracter-personal; última consulta 08/04/2020)

Navas Navarro, S. "Derecho e inteligencia artificial desde el diseño. Aproximaciones", en Navas Navarro. S (Dir) *Inteligencia Artificial. Tecnología y Derecho*, Tirant lo Blanch, Valencia, 2017.

Rodríguez, J. P., "El proceso de constitucionalización de una exigencia ética fundamental: el derecho a la intimidad", *Revista del Instituto Bartolomé de las Casas*, 1994, pp- 363-392.

Terrón Santos, D., Domínguez Álvarez, J., "Ley Orgánica 3/2018, De 5 de diciembre, de Protección de Datos y garantía de los Derechos Digitales", *AIS: Ars Iuris Salmanticensis,* vol. 7, nº 1, 2019, pp- 233-237.

Vergouw, B., Nagel, H., Bondt, G y Custers, B. "Drone Technology: Types, Payloads, Applications, Frequency Spectrum Issues and Future Developments", en Custers, B. (Ed), *The Future of Drone Use: Opportunities and Threats From Ethical and Legal Perspectives*, Springer, Amsterdam, Paises Bajos, 2016.

Warren, S.D. y Brandeis, L.D., "The Right to Privacy", *Harvard Law Review*, vol. 4, 1890.

Werrel, K.P., Stevends, D.D., "The evolution of cruise missile", Air University Press, Washington DC, 1985.

Whittle, R., "Predator: the secret origins of the drone revolution", Henry Holt and Co, Nueva York, 2014.

Winkler, S., Zeadally, S., y Evans, K. "Privacy and civilian drone use: the need for further regulation", *IEEE Security & Privacy*, vol. 16, nº5, 2018, pp. 72-80.

Yenne, B., "Attack of drones: a history of unmanned aerial combat", Zenith Press, St Paul, 2004.

Zaloga, S. J., "Unmanned aerial vehicles: robotic air warfare 1917-2007", Osprey Publishing, Oxford, 2008.