

**CAPÍTULO XII**

**OBLIGACIONES DEL OPERADOR EN MATERIA  
DE PROTECCIÓN DEL HONOR, LA INTIMIDAD  
PERSONAL Y FAMILIAR, LA PROPIA IMAGEN  
Y LOS DATOS DE CARÁCTER PERSONAL  
[ART. 26.F)]. COMPETENCIAS DE LA AEPD (ART. 7.3)**

Patricia MÁRQUEZ LOBILLO

Profesora Contratada Doctora de Derecho mercantil  
Acreditada al Cuerpo de Profesores Titulares de Universidad  
Universidad de Málaga

**SUMARIO:** I. SOBRE EL CONTENIDO DEL ART. 26.F): ¿PARA ESTE VIAJE HACÍAN FALTA ALFORJAS?:

1. Una mera remisión legislativa no es suficiente: la demanda de un régimen jurídico *ad hoc*. 2. El potencial de las aeronaves pilotadas por control remoto para realizar operaciones que puedan conculcar los derechos que analizamos. 3. Régimen jurídico aplicable a la protección del honor, de la intimidad personal y familiar, de la propia imagen y de los datos de carácter personal cuando se captan y tratan datos en operaciones con aeronaves pilotadas por control remoto. 4. Las competencias de la AEPD: referencia a una nueva e innecesaria remisión legislativa.—II. LA DETERMINACIÓN DEL SUJETO RESPONSABLE: BREVE PERO NECESARIA MENCIÓN.—III. LAS OBLIGACIONES DEL OPERADOR EN MATERIA DE PROTECCIÓN CIVIL DEL HONOR, LA INTIMIDAD PERSONAL Y FAMILIAR Y LA PROPIA IMAGEN.—IV. LA PROTECCIÓN DE DATOS PERSONALES CAPTADOS Y TRATADOS EN OPERACIONES CON AERONAVES PILOTADAS POR CONTROL REMOTO: 1. Consideraciones generales predicables tanto de las operaciones con aeronaves pilotadas por control remoto llevadas a cabo por «operadores privados» como de las efectuadas por «operadores públicos». 2. Especialidades de la protección de datos en «operaciones privadas» con aeronaves pilotadas por control remoto: examen del Reglamento General de Protección de Datos europeo. 3. Especialidades de la protección de datos en «operaciones públicas» con aeronaves pilotadas por control remoto: régimen actual y perspectivas de futuro: A) Régimen jurídico actual. B) La incorporación a nuestro ordenamiento de la DPD2016.

## I. SOBRE EL CONTENIDO DEL ART. 26.F): ¿PARA ESTE VIAJE HACÍAN FALTA ALFORJAS?

### 1. Una mera remisión legislativa no es suficiente: la demanda de un régimen jurídico *ad hoc*

La plena integración de las aeronaves pilotadas por control remoto en el espacio aéreo europeo se condiciona al establecimiento de un marco jurídico adecuado, que garantice un nivel de seguridad equivalente al previsto para las aeronaves pilotadas, tanto desde el punto de vista técnico como operacional o jurídico<sup>1</sup>.

En relación con este último aspecto y, en lo que a los efectos de este trabajo nos interesa, se impone la necesidad de consagrar los mecanismos necesarios para garantizar el respeto de los derechos al honor, la intimidad personal y familiar, la propia imagen y la protección de datos de carácter personal<sup>2</sup>.

A tal fin, no es suficiente, como hemos tenido oportunidad de poner de relieve<sup>3</sup>, tomando como referencia los pronunciamientos al respecto de las Instituciones comunitarias<sup>4</sup> o del Grupo de Trabajo Europeo sobre Protección de datos (GT29, en adelante)<sup>5</sup>, con aplicar sin más, de forma analógica, el régimen jurídico vigente en la materia. Si lo hiciéramos cometeríamos el error de no tomar en consideración la operación que se está desarrollando, el riesgo de la misma y/o la idoneidad de la aeronave para captar imágenes, sonidos,

<sup>1</sup> M.<sup>a</sup> J. GUERRERO LEBRÓN, «La regulación transitoria de los operadores de aeronaves civiles pilotadas por control remoto», *La Ley Mercantil*, 31 de julio de 2014; M.<sup>a</sup> J. GUERRERO LEBRÓN, C. CUERNO REJADO y P. MÁRQUEZ LOBILLO, «Aeronaves no tripuladas: estado de la legislación para realizar su integración en el espacio aéreo no segregado», *Revista de Derecho del Transporte. Terrestre, Marítimo, Aéreo y Multimodal*, núm. 12, 2013, pp. 63 y ss.; P. MÁRQUEZ LOBILLO, «Las aeronaves civiles pilotadas por control remoto en la Ley 18/2014, de 15 de octubre», *Revista de Derecho Mercantil*, núm. 294, 2014, pp. 425 y ss., y en «Consideraciones críticas sobre el régimen jurídico aplicable a las aeronaves civiles pilotadas por control remoto en el ordenamiento jurídico español», en J. I. PEINADO GRACIA (dir.) y M.<sup>a</sup> C. MAYORGA TOLEDANO (coord.), *Nuevos enfoques del Derecho aeronáutico y espacial*, Madrid, Marcial Pons, 2014, pp. 539 y ss.

<sup>2</sup> Derechos consagrados, como todos sabemos, en los arts. 7 y 8 de la Carta Europea de Derechos fundamentales, en el art. 16.1 del Tratado de Funcionamiento de la Unión Europea y en el art. 18 de nuestra Constitución.

<sup>3</sup> P. MÁRQUEZ LOBILLO, «Incidencia de la aprobación del Reglamento (UE) 2016/679 de 27 de abril de 2016 sobre la captura y tratamiento de datos personales en operaciones con drones», *La Ley Mercantil*, núm. 28, septiembre de 2016 (La Ley 6762/2016).

<sup>4</sup> Destacamos la Comunicación de la Comisión Europea al Parlamento Europeo y al Consejo, «Una nueva era en la aviación. Abrir el mercado de la aviación al uso civil de sistemas de aeronaves pilotadas de forma remota de manera segura y sostenible», COM (2014) 207 final, de 8 de abril; la Comunicación de la Comisión Europea al Parlamento Europeo, al Consejo Social, al Comité Económico y Social Europeo y al Comité de las Regiones, «Una estrategia de aviación para Europa», COM (2015) 598 final, de 7 de diciembre. *Vid.* además, R. L. FINN, D. WRIGHT, L. JACQUES y P. DE HERT, *Study on privacy, data protection and ethical risks in civil Remotely Piloted Aircraft Systems operations (Final Reports)*, 2014, pp. 257 y ss., elaborado a requerimiento de la Comisión Europea.

<sup>5</sup> Al examen de las exigencias del Grupo de Trabajo Europeo sobre Protección de datos en su «Opinión 1/2015, on Privacy and Data Protección Issues relating to utilisation of drones», de 29 de junio de 2015, hemos dedicado nuestro trabajo en P. MÁRQUEZ LOBILLO, «La era de los drones y su incidencia en la protección de los datos de carácter personal (A propósito de la Opinión 1/2015 del Grupo Europeo de Protección de Datos)», en M. FOLCHI (dir.), *ALADA en Bilbao*, Argentina, 2016.

datos personales, en condicionales tales que conculquen los derechos que analizamos.

Se impone la necesidad de elaborar normas específicas<sup>6</sup>, destinadas no solo a configurar las condiciones de aeronavegabilidad, sino también a fijar las reglas especiales para contribuir a garantizar el respeto a los derechos fundamentales que analizamos, «de conformidad con los principios de necesidad y proporcionalidad»<sup>7</sup>, tomando como referencia los conceptos de protección de la intimidad desde el diseño y por defecto, de tal forma que contribuyan «a la correcta aplicación de la normativa en materia de privacidad y protección de datos». Se destaca, además, la conveniencia de garantizar «que se informe a toda persona que maneje un RPAS de las normas básicas aplicables a la utilización de estos sistemas, y de que dichas normas deberían indicarse en un aviso para los compradores»<sup>8</sup>.

Estas ideas subyacen, de alguna forma, en la propuesta de futuro Reglamento europeo regulador de las operaciones con RPAS, elaborada por EASA, y que se debate actualmente en el seno de las instituciones comunitarias, con vistas a su aprobación en 2019<sup>9</sup>. En la misma se reconoce que la protección de la privacidad, de los datos personales y de la seguridad constituye un elemento esencial para la integración de RPAS, imponiéndose la necesidad de garantizar un marco jurídico centrado en la operación, proporcionado y que tome como referencia el riesgo de la misma (Considerando 12). Se consagra, como no puede ser de otra forma, pues en definitiva son aeronaves y son operadores aéreos, la obligación de respeto a las disposiciones reguladoras de la materia<sup>10</sup>, no sin prever mecanismos específicos que contribuyan al cumplimiento del objetivo legislativo propuesto. Entre ellos se citan el registro de la aeronave<sup>11</sup>; la identificación electrónica<sup>12</sup>; la implantación de mecanismos de *geofencing*<sup>13</sup>; la restricción de

<sup>6</sup> Que combinen las emanadas del poder legislativo con aquellas que nacen de la propia industria (códigos de conducta, cartas de privacidad...), *vid.* Dictamen del Comité Económico y Social Europeo sobre la Comunicación COM (2014) 207 final, aprobado en la sesión de 15 de octubre de 2014; y, Riga Declaration on «Remotely Piloted Aircraft (drones), Framing the future of aviation», de 6 de marzo de 2015.

<sup>7</sup> Parlamento Europeo, «Resolución sobre el uso seguro de los sistemas de aeronaves pilotadas de forma remota (RPAS), comúnmente conocidos como vehículos aéreos no tripulados (UAV), en el ámbito de la aviación civil [2014/2243(INI)]», de 29 de octubre de 2015 [P8\_TA-PROV(2015)0390].

<sup>8</sup> La EASA propone, en este sentido, la creación de un sitio web en el que se incorporen las disposiciones correspondientes, *vid.* «Concept of Operations for Drones. A risk based approach to regulation of unmanned aircraft», mayo de 2015. Al documento puede accederse a través del siguiente enlace: <https://www.easa.europa.eu/document-library/general-publications/concept-operations-drones>.

<sup>9</sup> European Aviation Safety Agency, Notice of Proposed Amendment 2017-05 (A), «Introduction of a regulatory framework for the operation of drones Unmanned aircraft system operations in the open and specific category», RMT.0230, de 4 de mayo de 2017, apdo. 2.3.1.4, al que se puede acceder en el siguiente enlace <https://www.easa.europa.eu/document-library/notices-of-proposed-amendment/npa-2017-05>.

<sup>10</sup> *Id.* art. 3. Respeto que se lleva al extremo de imponer, para determinadas operaciones y aeronaves, la obligación de que el operador y el piloto garanticen el conocimiento de dichas disposiciones.

<sup>11</sup> Obligatorio en prácticamente toda la tipología de aeronaves que contempla, como medio idóneo para poder localizar e identificar a su operador.

<sup>12</sup> Impuesto en atención al tipo de RPAS (equipados con sensores de audio o cámaras de más de cinco megapíxeles, o con un enlace de transmisiones de vídeo en tiempo real o cualquier otro sensor capaz de grabar datos personales) o por la zona en la que se está desarrollando la operación.

<sup>13</sup> Que impiden, por ejemplo, el acceso a determinadas zonas, o que permiten fijar claramente el posicionamiento de la aeronave.

zonas de vuelo por razones de seguridad y/o privacidad; la prohibición de volar en zonas donde ha acaecido una catástrofe; o la obligación del piloto de determinadas RPAS de conocer las normas más relevantes en materia de seguridad y protección de datos.

A pesar de lo expuesto, nuestro legislador no ha considerado conveniente establecer un régimen jurídico específico que contribuya a garantizar un nivel adecuado de protección de los derechos fundamentales que analizamos, y que sea, como exige el Parlamento Europeo, necesario y proporcionado. Se limita a solventar el problema por vía de la mera remisión legislativa, imponiendo al operador, en el art. 26.f) del RD-L de 15 de diciembre de 2017<sup>14</sup>, la obligación de:

«Adoptar las medidas necesarias para garantizar el cumplimiento de lo dispuesto en materia de protección de datos personales y protección de la intimidad en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y 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, sus normas de desarrollo y normativa concordante».

Es más, no se ha preocupado siquiera de establecer, en el ámbito de las operaciones que regula, qué medidas se consideran necesarias y cómo han de adoptarse para cumplir el mandato legislativo, lo que nos obliga a concretarlas tomando como referencia el régimen general en la materia.

Si tuviéramos que dar respuesta a la duda con la que encabezamos este epígrafe diríamos, sencillamente, que para este viaje no hacían falta alforjas. El operador de aeronaves pilotadas por control remoto, como el de aeronaves pilotadas<sup>15</sup>, como cualquier sujeto que capte o trate datos personales, del tipo o naturaleza que sean, deberá cumplir el régimen que analizaremos a continuación, se diga expresamente o se omita referencia alguna al respecto.

## **2. El potencial de las aeronaves pilotadas por control remoto para realizar operaciones que puedan conculcar los derechos que analizamos**

Aunque somos conscientes de las innumerables ventajas que pueden derivarse del uso de aeronaves pilotadas por control remoto, lo somos también de la potencial utilización de las mismas en operaciones que pueden conculcar los

<sup>14</sup> RD 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 RD 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 RD 57/2002, de 18 de enero, por el que se aprueba el Reglamento de Circulación Aérea (en adelante nos referiremos al mismo como el RD 1036/2017).

<sup>15</sup> Sobre la aplicación por el legislador del principio de equivalencia funcional y la conveniencia del mismo en el ámbito de las aeronaves pilotadas por control remoto, nos remitimos a I. QUINTANA CARLO, «El régimen jurídico de las aeronaves pilotadas por control remoto (RPAS): una interpretación en clave de Derecho privado», *Aequitas virtual. Revista de la Facultad de Ciencias Jurídicas de la Universidad del Salvador*, 2016, disponible en <http://p3.usal.edu.ar/index.php/aequitasvirtual/article/view/3746>.

derechos al honor, la intimidad personal y familiar, la propia imagen y los datos de carácter personal.

Sea por la facilidad que tienen para volar de forma casi clandestina; sea porque su reducido tamaño físico, en algunos casos, es un elemento que propicia aún más dicha clandestinidad; sea porque, son especialmente idóneas para llevar incorporados mecanismos que permitan la captación de datos personales, en un volumen y con una nitidez y calidad asombrosos<sup>16</sup>; sea porque estamos ante una tecnología que ofrece oportunidades por el momento desconocidas, etcétera.

Es evidente que cuando dichas operaciones se llevan a cabo en zonas pobladas, sobre personas, incluso con los estrictos márgenes legislativos en los que se pueden desarrollar tales operaciones, los problemas en orden a la materia que analizamos pueden verse agravados, ya no solo en los casos en los que la finalidad de la operación sea captar imágenes o datos de carácter personal, sino y sobre todo, en aquellos en los que la captación y/o el tratamiento de los mismos es incidental.

Como ha puesto de relieve de forma expresa el GT29, en su Dictamen de 2015, el uso de estas aeronaves resulta propicio para llevar a cabo una excesiva e ilícita recopilación de datos, para posibles usos multipropósito. Decimos excesiva e ilícita porque dicha captación de datos e imágenes puede efectuarse contraviniendo los pilares sobre los que se sustenta la protección de los derechos que analizamos, que serán expuestos a continuación (consentimiento, conocimiento, información, licitud, mínima injerencia, proporcionalidad, justificación, etcétera).

Y ello es así sencillamente porque los RPAS son técnicamente idóneos para ello<sup>17</sup>. Por mencionar algunas opciones<sup>18</sup>, pueden llevar incorporadas, incluso como elemento imprescindible para realizar la operación (pensemos en las funciones de observación, supervisión y vigilancia) tecnologías especialmente aptas para la captación de imágenes y sonidos (equipos de grabación, radares, equipos de radiofrecuencia, etc.), con una nitidez y resolución sorprendentes. Pueden portar cámaras especiales que permiten ver más allá de las fronteras que

---

<sup>16</sup> Así lo ha reconocido, de forma expresa, la Comisión de Libertades Civiles, Justicia y Asuntos de Interior en su «Opinión sobre el uso seguro de los sistemas de aeronaves dirigidas por control remoto (RPAS), comúnmente conocidos como vehículos aéreos no tripulados (UAV) en el ámbito de la aviación civil», de 30 de septiembre de 2015, citada anteriormente, afirmando la ponente que a pesar de los beneficios de dichas aeronaves, «su utilización conlleva riesgos significativos, en concreto porque los RPAS permiten mejorar otras tecnologías que pueden usarse para la vigilancia y el seguimiento de personas y bienes [...] que son por definición una tecnología de doble uso que requiere unas normas muy estrictas y rigurosas; que el uso de RPAS también plantea una serie de retos específicos cuando implica el tratamiento de datos personales, ya que ello interfiere con derechos fundamentales, en particular el derecho a la vida privada y el derecho a la protección de datos, y cuando afecta a la seguridad pública, ya que los RPAS pueden ser utilizados, ya sea de manera intencionada o no intencionada, para infligir daños a personas e infraestructuras».

<sup>17</sup> El GT29, en su Opinión 1/2015, lo pone de relieve señalando un inconveniente de las operaciones con RPAS, predicable especialmente de aquellas que se llevan a cabo con la finalidad que hemos denominado pública, que resume de forma sumamente gráfica toda la problemática que planteamos: «*This will result in an increased feeling of being under surveillance and a subsequent possible decrease in the legitimate exercise of civil liberties and rights, best known as "chilling effect"*».

<sup>18</sup> Vid. R. L. FINN, D. WRIGHT, L. JACQUES y P. DE HERT, *Study on privacy, data protection and ethical risks in civil Remotely Piloted Aircraft Systems operations...*, op. cit. pp. 257 y ss.

imponen los muros o paredes (infrarrojos). Pueden estar dotados de programas informáticos que permitan el reconocimiento facial o biométrico en tiempo real, conforme a los parámetros con los que hayan sido programados. Pueden llegar a lugares insospechados, alcanzando puntos de observación únicos y prácticamente sin límites espaciales. Pueden interconectarse formando un «enjambre de drones», que facilita un mayor espectro de actuación y la vigilancia coordinada de un mayor espacio. Determinados RPAS son, además, prácticamente invisibles dado su tamaño, lo que les permite ocultarse fácilmente en vuelo, moverse con gran facilidad y sobrevolar espacios aéreos, de mayor o menor dimensión, en función de la aeronave que se esté utilizando para ello<sup>19</sup>.

No estamos diciendo que por el mero hecho de llevar incorporada dicha tecnología los RPAS sean peligrosos. Es obvio que nos referimos al uso que pueda hacerse de los mismos, y es que puede que incluso por desconocimiento del operador se lleven a cabo captaciones, no conocidas y no consentidas, públicas o privadas, que pueden suponer un atentado a la intimidad y a la privacidad de las personas, siempre, como es obvio, que la misma se realice conculcando las disposiciones legales en la materia.

Es más, no solo se van a plantear problemas en los supuestos en los que las captaciones sean efectuadas por particulares. Van a ser incluso mayores cuando se empleen aeronaves pilotadas por control remoto en el ejercicio de funciones de vigilancia, control de fronteras, seguridad, etc., llevadas a cabo por autoridades competentes. De hecho, especiales problemas o riesgos se acusan por el GT29 en su Opinión 1/2015, en los supuestos de captaciones realizadas con fines públicos (prevención de la delincuencia, garantía de la seguridad ciudadana, control del tráfico viario, control de fronteras, control aduanero, etc.), sobre todo por los nefastos efectos que pueden derivarse del uso intrusivo de aeronaves no pilotadas, de su empleo para la vigilancia indiscriminada de personas, del tratamiento analítico de datos o de la puesta en común de dichos datos para el trazado de perfiles<sup>20</sup>.

### **3. Régimen jurídico aplicable a la protección del honor, de la intimidad personal y familiar, de la propia imagen y de los datos de carácter personal cuando se captan y tratan datos en operaciones con aeronaves pilotadas por control remoto**

La ausencia de un régimen jurídico específico para la protección de los derechos fundamentales que analizamos, cuando se captan y tratan datos personales en operaciones con aeronaves pilotadas por control remoto, nos obliga a concre-

<sup>19</sup> Todas estas utilidades han sido puestas de relieve en la Opinión 1/2015, del Grupo de Trabajo Europeo sobre Protección de datos, en su apdo. 2. De forma detallada, en la doctrina, E. ACED FÉLEZ, «Drones: una nueva era de la vigilancia y la privacidad», *Red Seguridad. Revista especializada en protección de datos, informática y comunicaciones*, núm. 60, marzo de 2013, pp. 48 y 49, disponible en el siguiente enlace: <http://www.redseguridad.com/revistas/red/060/index.html?#/6/>.

<sup>20</sup> Para evitar reiteraciones innecesarias, nos remitimos a P. MÁRQUEZ LOBILLO, «La era de los drones y su incidencia en la protección de los datos de carácter personal (a propósito de la Opinión 1/2015...», *op. cit.*, *passim*.

tar el mismo. No porque, como afirmamos, haya diferencias con cualquier otro sujeto que capte y/o trate datos personales, sino por las deficiencias de las que adolece el régimen previsto en el art. 26.f) del RD 1036/2017.

La remisión legislativa con la que nuestro legislador zanja el problema que analizamos, *ex* LOPD, la LO 1/1982 y concordantes<sup>21</sup>, se presenta, como mínimo, incompleta para cumplir el objetivo de garantizar un adecuado nivel de protección de los derechos fundamentales al honor, la intimidad personal y familiar, la propia imagen y la protección de los datos personales.

Tal afirmación se fundamenta, en primer lugar, en el examen de la tipología de operaciones y operadores que contempla nuestro legislador en el RD 1036/2017.

Así, tomando como referencia lo establecido en su art. 2, podemos diferenciar dos tipos de operadores y operaciones susceptibles de realizarse con RPAS, en lo que a nosotros nos concierne. Aquellas que llevan a cabo «operadores privados», cualquier empresario o profesional que opere aeronaves pilotadas por control remoto para la realización de la tipología de vuelos que la norma contempla<sup>22</sup>; y operaciones que se efectuarán por «sujetos públicos» en el ámbito de sus funciones específicas de policía, aduanas, salvamento, bomberos, guardacostas, control viario, servicios de inteligencia, etcétera<sup>23</sup>.

El carácter incompleto de la norma se acusa porque, respecto de las primeras, resultará plenamente aplicable la remisión legislativa, pero, en relación con las segundas no. De hecho, están expresamente excluidas del ámbito de aplicación de las normas a las que el RD 1036/2017 se remite<sup>24</sup> o amparadas en las excepciones que dichas disposiciones contienen<sup>25</sup>. No encontramos en el Texto referencia alguna al régimen aplicable a la protección de los derechos que analizamos cuando se operan RPAS por «operadores públicos», ni consideramos que la misma deba entenderse hecha en la remisión genérica a las concordantes.

<sup>21</sup> Incluiría, entendemos, el RLOPD y la LO 1/1996 de 15 de enero, de Protección Jurídica del Menor.

<sup>22</sup> Es más, vista la tipología de operaciones que se contemplan en el art. 5 consideramos más que probable que las conductas contrarias a los derechos fundamentales que analizamos se realicen cuando se efectúan operaciones aéreas especializadas, al menos de manera intencional. En los supuestos de vuelos experimentales, vemos más probable que se pueda producir una captación de naturaleza incidental, debiendo los operadores establecer mecanismos que, de alguna forma, permitan evitarla y/o, en caso de captarse los datos, que los mismos puedan ser destruidos en el más breve periodo de tiempo.

<sup>23</sup> Así las diferencia el GT29, de hecho, en su Opinión 1/2015, previendo, incluso, un régimen de obligaciones distinto en función de la naturaleza, privada o pública, de la operación que se esté desarrollando con la aeronave pilotada por control remoto.

<sup>24</sup> *Ex. arts. 2.3.e) y 22 de la LO 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD) vigente actualmente. Se excluyen, igualmente, del ámbito de aplicación del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), DOUE L 119/1, de 4 de mayo de 2016 (en adelante, RGPD). Vid., además, la DT 4.ª del Proyecto de Ley Orgánica de Protección de datos de carácter personal (PLOPD), de 24 de noviembre de 2017. El texto del mismo puede consultarse en el siguiente enlace: [http://www.congreso.es/public\\_oficiales/L12/CONG/BOCG/A/BOCG-12-A-13-1.PDF](http://www.congreso.es/public_oficiales/L12/CONG/BOCG/A/BOCG-12-A-13-1.PDF).*

<sup>25</sup> *Vid. arts. 2 y 8 de la LO 1/1982.*

El legislador debería haberse remitido, al menos<sup>26</sup>, a lo previsto en la Decisión Marco 2008/977/JAI del Consejo<sup>27</sup>; en el RD de 14 de septiembre de 1882, por el que se aprueba la Ley de Enjuiciamiento Criminal; en LO 4/2015, de 30 de marzo, de protección de la seguridad ciudadana; y, en la LO 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las fuerzas y cuerpos de seguridad en lugares públicos. Régimen jurídico aplicable, en nuestra opinión, a la captación y tratamiento de imágenes y otros datos de carácter personal, cuando se realizan las operaciones contempladas en el RD 1036/2017 por parte de los que hemos denominado «operadores públicos», en el ejercicio de las funciones que les son propias, como tendremos oportunidad de analizar en este trabajo.

No es solo la insuficiente remisión legislativa o la deficiencia de la misma el motivo por el que consideramos que el contenido del art. 26.1.f) que tratamos es incompleto. El legislador yerra al omitir referencia a los mecanismos específicos para garantizar el cumplimiento de las obligaciones en la materia y evitar sanciones.

Se nos vienen a la mente, por ejemplo, las dificultades en orden al cumplimiento de los deberes de información cuando se operan aeronaves pilotadas por control remoto de menos de 2 kg de MTOM, que fueron puestas de relieve por el GT29, con mención expresa de los posibles cauces para solucionarlas, y que no han sido tomados en consideración por el legislador español.

No podemos olvidar, por otro lado, que a la fecha de aprobación del RD 1036/2017, ya se encontraba en vigor el RGPD<sup>28</sup>, aunque el mismo no sea plenamente aplicable hasta el 28 de mayo de 2018, por lo que dada la dificultad del mismo y su carácter general, no hubiera estado mal la concreción de dichos mecanismos tomando como referencia la norma comunitaria y de forma específica para este ámbito<sup>29</sup>. En aplicación del principio de primacía del Dere-

---

<sup>26</sup> En la defensa que hacemos de normas *ad hoc* bien podría haber aprovechado la oportunidad e incorporado a nuestro ordenamiento las normas específicas que permitan dar cumplimiento a las obligaciones que pudieran derivarse de la Directiva (UE) 2016/680, del Parlamento Europeo y del Consejo, de 27 de abril, 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 (en adelante DPD2016). La transposición de la norma, obligatoria para el 6 de mayo de 2018, está prevista, en el Plan Anual normativo de 2018, como se puede comprobar en el siguiente enlace: [http://www.lamoncloa.gob.es/consejodeminstros/referencias/documents/2017/refc20171207e\\_2.pdf](http://www.lamoncloa.gob.es/consejodeminstros/referencias/documents/2017/refc20171207e_2.pdf).

<sup>27</sup> Decisión Marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal.

<sup>28</sup> Aunque es obvio que el objetivo del legislador comunitario no era regular el tratamiento de datos personales captados en operaciones con drones, hay voces que afirman que, en determinados casos, parece que está pensando en ellas. Así F. J. SEMPERE SAMANIEGO, *Comentarios prácticos a la Propuesta de Reglamento de Protección de Datos de la Unión Europea*, 2013, p. 305, disponible en [http://www.privacidadlogica.es/wp-content/uploads/2013/09/comentarios-reglamento-pdatos\\_Javier-Sempere-Samaniego.pdf](http://www.privacidadlogica.es/wp-content/uploads/2013/09/comentarios-reglamento-pdatos_Javier-Sempere-Samaniego.pdf).

<sup>29</sup> A falta de dicha concreción, no parece quedar otra al operador que analizar con detenimiento el considerable número de documentos-guías elaborados por la AEPD, con el objetivo de contribuir a un mejor entendimiento de esta complicada norma. Nos referimos, por mencionar los más relevantes o básicos, a la «Guía del Reglamento General de Protección de datos para responsables del tratamiento»; la «Guía sobre el cumplimiento del deber de informar»; «Orientaciones y garantías en los procedimientos

cho comunitario<sup>30</sup> debemos entender que la protección del tratamiento de datos personales en las operaciones con aeronaves no pilotadas habrá de acomodarse a la norma comunitaria, entendiéndose tácitamente derogada la LOPD y su normativa de desarrollo en todo aquello que difiera o contravenga el contenido del Texto europeo<sup>31</sup>. Es obvio, por ello, que abordaremos la materia tomando como referencia el RGPD.

#### **4. Las competencias de la AEPD: referencia a una nueva e innecesaria remisión legislativa**

Coherente con el proceder legislativo y la solución de los problemas en orden a la protección de los datos personales por vía de remisión, nuestro legislador, en el art. 7.3 del RD 1036/2017 salva las competencias de la AEPD, en lo que a labores de supervisión y control se refiere, como es obvio en el ámbito que le es propio.

El legislador europeo ha fijado, en el art. 83 RGPD las condiciones generales aplicables a la imposición de sanciones administrativas, sobre la base de los principios de efectividad, proporcionalidad y con finalidad disuasoria, correspondiendo a las autoridades nacionales (AEPD) la garantía del cumplimiento de dichos principios. Se contempla que la imposición de las multas se realice a título adicional o sustitutivo de las medidas contempladas en el art. 58.2.a), h) y j), teniendo en cuenta los criterios o elementos para la graduación que la norma prevé y a los que nos remitimos.

Si merece la pena referenciar el importe máximo de las sanciones en el caso de incumplimiento por el responsable y el encargado de sus obligaciones, que podrá alcanzar la cifra de 20 millones de euros o el 4 por 100 del volumen de negocios, si es mayor, conforme a lo previsto en los apdos. 4 y ss. del art. 83.

Prevé el legislador en el art. 84 RGPD, además, la competencia de los Estados miembros para establecer las normas en materia de otras sanciones apli-

---

de anonimización de datos personales»; o su «Guía para una Evaluación de Impacto en la Protección de Datos Personales (EIPD)-2014». El texto de todos ellos, junto al de algún otro al que aludiremos, se encuentra disponible en el siguiente enlace: <http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/index-ides-idphp.php>.

<sup>30</sup> Sobre el que podemos encontrar un interesante y reciente trabajo en J. AÑÓN CALVETE, «Primacía del Derecho de la Unión Europea (a propósito de la STC 232/2015, de 5 de noviembre)», *Noticias Jurídicas*, 22 de febrero de 2016, disponible en <http://noticias.juridicas.com/conocimiento/articulos-doctrinales/10895-primacia-del-derecho-de-la-union-europea-a-proposito-de-la-stc-232-2015-de-5-de-noviembre/>.

<sup>31</sup> Como hemos anunciado anteriormente, a la fecha del presente trabajo, con plazo de enmiendas ampliado a 6 de febrero de 2018, se está preparando el PLOPD, por el que se pretende la adaptación del régimen español al RGPD, completando sus disposiciones en todos aquellos aspectos en los que la norma comunitaria lo permite (art. 1 PLOPD). La forma en la que se presenta el texto nos merece, como mínimo, sorpresa. El legislador español realiza, en prácticamente todo el articulado, remisiones a la norma europea, cuando en nuestra opinión no hubiera sido necesario y hubiera sido mucho más conveniente y con mejor técnica legislativa una disposición en la que se limitase a regular aquellos aspectos que le reserva el RGPD sin remisión al número del precepto, transcribiéndolo o explicando el objeto de la norma concreta. A más claridad, sin duda, contribuiría. Nos veremos abocados al manejo de ambas disposiciones a la vez para conocer con plenitud el régimen jurídico aplicable a la protección de datos de carácter personal.

cables a las infracciones del Reglamento, en particular, las que no se sancionen conforme al art. 83<sup>32</sup>. Deberán, además, prever las medidas para garantizar su observancia y respetar, en la fijación, los principios de disuasión, efectividad y proporcionalidad. Este régimen deberá ser notificado a la Comisión.

## II. LA DETERMINACIÓN DEL SUJETO RESPONSABLE: BREVE PERO NECESARIA MENCIÓN

Conforme a lo establecido en el art. 26.f) del RD 1036/2017, las obligaciones en materia de protección de los derechos que analizamos recaen sobre el operador, definido en el art. 5.i) de la norma, quien tendrá, en el ámbito que nos ocupa, la condición de responsable del tratamiento (art. 4.7 RGPD o art. 3.8 DPD2016)<sup>33</sup>. La referencia al mismo tiene, en este capítulo, una doble finalidad.

La primera, como es obvio, conocer quien es el sujeto responsable del cumplimiento de las exigencias en materia de protección del honor, de la intimidad personal y familiar y de la propia imagen, así como, de las relativas a la protección de los datos tratados, en orden, como no puede ser de otra forma, a imputarle las oportunas responsabilidades por el incumplimiento de las mismas, y a los efectos de determinar ante quien pueden ser ejercitados los derechos que las normas contemplan.

La segunda, aunque pueda parecer innecesaria, para recordar el limitado ámbito de aplicación del RD 1036/2017, y poner de manifiesto que, el cumplimiento de los obligaciones en materia de protección de los derechos que analizamos no deriva de la remisión legislativa, sino de la existencia de normas *ad hoc*, aplicables a cualquier sujeto que opere en el mercado de las aeronaves pilotadas por control remoto, con independencia de que la operación que desa-

<sup>32</sup> Vid. arts. 70 y ss. del PLOPD, en los que el prelegislador cataloga el régimen de los incumplimientos de la norma conforme a criterios de gravedad, fija los plazos prescriptivos, amplía el elenco de circunstancias a tener en cuenta para graduar las sanciones, etc., siempre tomando como referencia la norma Comunitaria.

<sup>33</sup> Para diferenciarlo del encargado del mismo, que será aquel sujeto que trate los datos por cuenta del responsable (art. 4.8 RGPD o art. 3.9 DPD2016). La relación de ambos, sobre la base de los pilares o exigencias del art. 22 RDPD o del art. 22 DPD2016, centrados en definitiva en que el tratamiento deba encomendarse a encargados cualificados y que cuenten con las medidas técnicas y las garantías suficientes para ejercer sus funciones, habrá de plasmarse en un contrato que contendrá como mínimo las estipulaciones del art. 22.5 RGPD (*vid.* art. 33.2 PLOPD) o del art. 22.3 DPD2016. Sobre la forma en la que ha de elaborarse dicho contrato, el 26 de enero de 2017, la AEPD elaboró sus «Directrices para la elaboración de contratos entre responsables y encargados de tratamiento», a las que se puede acceder en el siguiente enlace: <https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/directricescontratos.pdf>.

Las obligaciones del mismo son equiparables a las que asume el responsable, por lo que nos remitimos a todo lo que analizaremos en relación con el operador-responsable en este trabajo. La AEPD los ha incluido, de hecho, en la misma Guía explicativa ([https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia\\_responsable\\_ficheros.pdf](https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_responsable_ficheros.pdf)). También consideramos conveniente enlazar la Guía específica elaborada por la autoridad de protección de datos catalana ([http://apd-cat.gencat.cat/web/.content/03-documentacio/Reglament\\_general\\_de\\_proteccio\\_de\\_dades/documents/Guia-encargado-del-tratamiento-RGPD-CAST.pdf](http://apd-cat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/documents/Guia-encargado-del-tratamiento-RGPD-CAST.pdf)). Aunque anterior al texto, no podemos olvidar que esta figura ya aparecía prevista en el régimen anterior al mismo, merece la pena referenciar, el «Dictamen 1/2010 sobre los conceptos de “responsable del tratamiento” y “encargado del tratamiento”», del GT29, de 16 de febrero de 2010.

rolle esté o no comprendida en el ámbito de aplicación de la norma que comentamos. Precisión que entendemos conveniente dado el contenido de su art. 1.2 y la posibilidad que el mismo prevé de que se autoricen por AESA otro tipo de operaciones; o dada la exclusión de los vuelos desarrollados en su integridad en espacios interiores completamente cerrados, en los que siguen imperando los principios protectores de los derechos que analizamos<sup>34</sup>.

Respecto de la concreción del sujeto responsable, con remisión expresa al Capítulo III de esta obra colectiva, solo una puntualización más.

En el supuesto de «operaciones privadas» llevadas a cabo por «operadores privados», estaremos a lo establecido en el art. 5.i) del RD 1036/2017.

En el caso de «operaciones públicas», desarrolladas por «operadores públicos», no podemos olvidar las previsiones contenidas en el art. 3.2, párrafos 2.º y 4.º, en orden a las funciones, competencias y responsabilidades que asume el organismo público que autorice la operación, a quien compete, asegurarse de que la misma pueda realizarse en condiciones de seguridad y de que cumple los requisitos que le son exigibles, incluidos, entendemos, los que impongan las normas sobre protección de los derechos fundamentales a los que dedicamos este trabajo. Dicho organismo público tiene, en nuestra opinión, la consideración de responsable del tratamiento, en el sentido de autoridad competente, a la que se refiere la LO 4/1997, o de autoridad pública competente, en palabras del legislador europeo en la DPD2016. El piloto al mando de la aeronave deberá tener, en nuestra opinión, y con las consecuencias que de ello se derivan, la condición de encargado del tratamiento.

### III. LAS OBLIGACIONES DEL OPERADOR EN MATERIA DE PROTECCIÓN CIVIL DEL HONOR, LA INTIMIDAD PERSONAL Y FAMILIAR Y LA PROPIA IMAGEN

La protección civil del honor, la intimidad personal y familiar y la propia imagen<sup>35</sup>, frente a todo tipo de intromisiones ilegítimas se lleva a cabo por el

<sup>34</sup> Queremos traer a colación, en este sentido, por la problemática que suscita, el posible uso de aeronaves no tripuladas en los lugares del trabajo, al amparo del art. 20.3 del Estatuto de los Trabajadores, como medida de control de la actividad laboral. El desarrollo con esa finalidad, exclusivamente, no requiere recabar el consentimiento de los trabajadores afectados. En cuanto al deber de información, la doctrina del Tribunal Constitucional ha pasado de la imposición de un deber estricto (Sentencia de 11 de febrero de 2013), a uno más laxo, siempre que se cumplan los principios básicos en materia de protección de datos (Sentencia de 3 de marzo de 2016). El Tribunal Europeo de Derechos Humanos, en su Sentencia de 12 de enero de 2016, si bien en un asunto de control de comunicaciones electrónicas, se muestra partidario de la corriente estricta. *Vid.* L. MELGAR MARTÍNEZ, «Trabajadores, medios tecnológicos y control empresarial», *Diario La ley*, 20 de diciembre de 2016.

<sup>35</sup> Estos derechos han sido calificados por el Tribunal Constitucional, en la Sentencia de 28 de enero de 2003, como autónomos y sustantivos, aunque estrechamente vinculados entre sí, en tanto que derechos de la personalidad, derivados de la dignidad humana y dirigidos a la protección del patrimonio moral de las personas. Excede del objeto de nuestro estudio el examen del contenido pormenorizado de cada uno de los derechos contemplados en el art. 18 de la Constitución Española. Nos remitimos, por ello, sin perjuicio de hacer referencia a alguna resolución que consideremos, a la sinopsis publicada en la página del Congreso (<http://www.congreso.es/consti/constitucion/indice/sinopsis/sinopsis.jsp?art=18&tipo=2>), en la que podremos encontrar los pronunciamientos base, tanto del Tribunal

procedimiento previsto en el art. 9 de la LO 1/1982, que se declara, expresamente, compatible con cualquier procedimiento penal, subrayando que el carácter delictivo de la intromisión no impide el recurso al procedimiento de tutela contemplado en esta Ley especial.

El ámbito de protección de la norma viene delimitado, *ex art. 2*, por las leyes y por los usos sociales, atendiendo al ámbito que, por sus propios actos, mantenga reservado cada persona para sí y su familia o, en palabras del Tribunal Supremo, en momentos o lugares que la mayoría de las personas reservamos para nosotros mismos sin exponerlos a la curiosidad ajena<sup>36</sup>.

No existirá, en consecuencia, intromisión ilegítima en aquellos supuestos en los que una norma legal la permita<sup>37</sup>, así como, en los casos en los que la conducta se haya llevado a cabo con consentimiento expreso<sup>38</sup> del titular del

---

Constitucional como del Tribunal Supremo hasta 2011, seguidos en la mayoría de las resoluciones posteriores. Destacamos, igualmente, los relativos a la inviolabilidad del domicilio o al secreto de las comunicaciones que dicha sinopsis contiene. En la doctrina, *vid.* recientemente J. R. DE VERDAD Y BEAMONTE, «Los derechos al honor, a la intimidad y a la propia imagen como límites del ejercicio de los derechos de información y expresión: ¿una nueva sensibilidad de los Tribunales?», *Derecho Privado y Constitución*, núm. 29, enero-diciembre de 2015, pp. 389 y ss.; P. ESCRIBANO TORTAJADA, «Drones y derecho a la intimidad: estado de la cuestión y problemas que se plantean en la actualidad», en M.ª J. GUERRERO LEBRÓN y J. I. PEINADO GRACIA (dirs.), e I. CONTRERAS DE LA ROSA (coord.), *El Derecho aéreo entre lo público y lo privado. Aeropuertos, acceso al mercado, drones y responsabilidad*, Sevilla, Servicio de Publicaciones de la UNIA, 2017, pp. 244 y ss.; J. MARTÍNEZ DE PISÓN, «El derecho a la intimidad: de la configuración inicial a los últimos desarrollos en la jurisprudencia constitucional», *Anuario de Filosofía del Derecho*, 2016, XXXII, pp. 409 y ss.; T. VÁZQUEZ RUANO, «Implicaciones legales de las aeronaves tripuladas por control remoto en el ámbito comercial. Protección de la información personal», *Revista de Derecho del Transporte. Terrestre, Marítimo, Aéreo y Multimodal*, núm. 17, 2016, pp. 151 y ss.

<sup>36</sup> Sentencia del Tribunal Supremo de 12 de septiembre de 2011. En los que quedarán protegidos, incluso, los personajes públicos, como puso de manifiesto el Tribunal Europeo de Derechos Humanos, en su Sentencia de 24 de junio de 2004, asunto *Von Hannover v. Alemania* y, más recientemente, en la de 21 de febrero de 2017, asunto *Rubio Dosamantes v. España*. En este sentido debemos traer a colación la importancia que los órganos jurisdiccionales dan al celo del titular de los derechos en la protección de los mismos, poniendo de relieve el Tribunal Supremo que se considera que existe intromisión ilegítima en aquellos supuestos en los que se captan imágenes en lugares solitarios, buscados a propósito por el lesionado para garantizarse su privacidad (así, Sentencias de 18 de noviembre de 2008 o de 23 de junio de 2015).

<sup>37</sup> Excepción que dará cabida a intromisiones en los derechos que analizamos llevadas a cabo en «operaciones públicas» con aeronaves pilotadas por control remoto en las condiciones que analizaremos en este mismo trabajo, y con la exclusiva finalidad de protección de la seguridad, prevención de la delincuencia, etcétera.

<sup>38</sup> Respecto del consentimiento de menores, nos remitimos a lo establecido en el art. 3 de la norma, recayendo la capacidad para otorgarlo en sus representantes legales, que habrán de ponerlo en conocimiento del Ministerio Fiscal, decidiendo en caso de oposición de este el órgano jurisdiccional. La jurisprudencia en torno a la prevalencia de los derechos de los menores a no ser grabados es bastante extensa, sobre todo en supuestos en los que se ha alegado el derecho a la información. Destacamos, en este sentido, el Auto del Tribunal Supremo de 20 de diciembre de 2017, en el que se reitera la doctrina de este Alto Tribunal, contenida, entre otras, en la importante Sentencia de 30 de junio de 2015, trayendo a colación la del Tribunal Constitucional de 29 de junio de 2009.

Excede de nuestro estudio, por otro lado, el examen de las específicas disposiciones relativas a la protección de los derechos que contempla la norma en el caso de personas fallecidas previstas en los arts. 4 a 6, a los que nos remitimos. Solo referenciar que no encontramos en el RD 1036/2017 disposición alguna que haga referencia a la imposibilidad de sobrevolar espacios en los que ha ocurrido un accidente o catástrofe, como sí se contiene en la Propuesta de Reglamento Europeo de EASA, de 2017, cuando la misma supone una importante garantía de los derechos de las personas afectadas por la misma y de sus familiares, en el sentido que prevé la LO 1/1982.

derecho<sup>39</sup>. Tampoco, en los supuestos en los que predomine un interés histórico, científico o cultural relevante (art. 8.1)<sup>40</sup>.

Atendiendo al concepto de intromisión ilegítima del art. 7, *a sensu contrario*, y por la naturaleza de las operaciones que pueden realizarse con las aeronaves que analizamos, el operador habrá de recabar el consentimiento expreso mencionado, en los supuestos en los que utilice aparatos de escucha, dispositivos ópticos o cualquier otro procedimiento que le permita conocer la vida íntima de las personas o captar su imagen<sup>41</sup> «en lugares o momentos de su vida privada o fuera de ellos, salvo los casos previstos en el artículo octavo, dos». De estas excepciones, destacamos, por razón de la materia, la captación que pueda realizarse de cargos públicos en actos públicos y lugares públicos, así como, las captaciones meramente incidentales, en sucesos o acontecimientos públicos, cuando la imagen de la persona aparezca como meramente accesoría.

#### IV. LA PROTECCIÓN DE DATOS PERSONALES CAPTADOS Y TRATADOS EN OPERACIONES CON AERONAVES PILOTADAS POR CONTROL REMOTO

##### 1. Consideraciones generales predicables tanto de las operaciones con aeronaves pilotadas por control remoto llevadas a cabo por «operadores privados» como de las efectuadas por «operadores públicos»

El examen del régimen jurídico aplicable a la protección de los datos de carácter personal, cuando se llevan a cabo captaciones y tratamientos en operaciones con aeronaves pilotadas por control remoto, ha de realizarse, en nuestra opinión, diferenciando según dichas operaciones sean desarrolladas por «operadores privados» u «operadores públicos».

Aunque así lo haremos, se observan coincidencias en dos elementos que trataremos de forma conjunta. El concepto de dato de carácter personal y la exigencia de que se produzca el tratamiento de los datos captados para que entre en funcionamiento la maquinaria tuitiva que proporciona el legislador en el RGPD y en la LO 4/1997, atendiendo a la finalidad privada o pública de la operación, respectivamente. Si la voluntad del legislador y su obligación es incorporar la

<sup>39</sup> Consentimiento que, por otro lado, será revocable en cualquier momento, sin perjuicio de que proceda la indemnización de los daños y perjuicios causados, así como de las expectativas que puedan ser justificadas.

<sup>40</sup> No quedarían amparados en la excepción de interés general, los supuestos que convierten en instrumentos de diversión y entretenimiento algo tan personal como los padecimientos o la misma muerte de un individuo, como puso de manifiesto el Tribunal Constitucional en una de las sentencias más relevantes en esta materia, la de 2 de diciembre de 1988. *Vid.* F. HERRERO-TEJEDOR ALGAR, «STC 231/1988, de 2 de diciembre: Caso “Paquirri”», en A. DORREGO DE CARLOS (COORD.), *Veinticinco años de jurisprudencia constitucional. 25 sentencias fundamentales comentadas*, Madrid, Grupo Difusión, 2007, pp. 107 y ss.

<sup>41</sup> En consonancia con el concepto de dato personal (*vid. infra*), entendemos que dicho consentimiento habrá de recabarse no solo cuando lo captado sea la imagen, sino también cualquier otro dato o elemento que, de forma directa o indirecta, permita la identificación de dicha persona.

DPD2016 en 2018, es evidente que nuestro trabajo, si no quiere quedar obsoleto, debe hacer las oportunas referencias al Texto europeo.

Otro elemento es trascendental en ambas disposiciones legales, y está íntimamente relacionado con el tratamiento. A él aludiremos en este apartado para dejar constancia de que no cualquier tratamiento es lícito y está permitido, que no todo es válido y que para proceder a tratar datos de carácter personal ha de acreditarse una clara y específica finalidad.

Entrando en el concepto de dato personal y, conforme a lo establecido en los arts. 4.1 RGPD o 3.1 DPD2016, nos estaremos refiriendo a «toda información sobre una persona física identificada o identificable», considerándose persona física identificable:

«toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona, cualquier información concerniente a las personas físicas, identificada o identificables, sea de carácter numérico, alfabético, gráfico, acústico o de cualquier otro tipo».

Se plasma, en definitiva, la conceptualización de dato de carácter personal contenida en la STC de 30 de noviembre de 2000, confirmada en la de 11 de febrero de 2013, entre otras.

El concepto de dato de carácter personal comprende, cualquier dato de una persona, sea íntimo o no, cuyo conocimiento por terceros pueda afectar a sus derechos, fundamentales o no.

«Por consiguiente, también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que solo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo».

Como ya había indicado el Tribunal Constitucional en su Sentencia de 4 de mayo de 1998, el objetivo de la protección de este derecho fundamental no es otro que garantizar a su titular el control sobre sus datos personales (cualesquiera que sean estos) y sobre el uso y destino de los mismos.

Conforme ha evolucionado la tecnología, como reconoce el legislador europeo en los Considerandos que acompañan al RGPD, ha evolucionado el propio concepto de dato de carácter personal, teniendo cabida en el mismo cualquier elemento que permita identificar a una persona, directa o indirectamente.

En el ámbito que nos ocupa, por la tipología de las operaciones a realizar con aeronaves pilotadas por control remoto, adquiere especial relieve la imagen como dato de carácter personal por entender que la misma no solo suministra

información sobre la persona, sino sobre el lugar en el que se ha captado su imagen y la actividad que está desarrollando<sup>42</sup>; los datos biométricos<sup>43</sup>, en tanto una vez captados y realizado el oportuno tratamiento es fácil proceder a la identificación de una persona y, especialmente, para poder averiguar aspectos conductuales de la misma que contribuyan a la creación de perfiles; los datos contenidos en los dispositivos inteligentes<sup>44</sup>, a los que fácilmente se puede acceder desde programas *ad hoc* instalados en la aeronaves, que permitan a la misma interconectarse con dichos dispositivo, etcétera.

La exigencia de que los datos captados sean objeto de tratamiento es predecible tanto de las captaciones en «operaciones públicas» como de las llevadas a cabo en «operaciones privadas». De hecho, la razón de ser de las normas europeas es, fundamentalmente, la protección frente a dicho tratamiento (art. 1 RGPD o art. 1 DPD2016).

Cuando hablamos de tratamiento nos estamos refiriendo a:

«cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción» (art. 4.2 RGPD o art. 3.2 DPD2016).

La finalidad del tratamiento constituye, por otro lado, un elemento fundamental, toda vez que no es lícito que el mismo se produzca con cualquier objetivo o razón y, además, va a servir de vía para determinar cuáles quedan sometidos al ámbito de aplicación de las disposiciones mencionadas y cuales excluidos.

En este sentido, en el ámbito de las «operaciones privadas», y sobre la base del principio de transparencia y la obligación de proporcionar una información detallada sobre los motivos que fundamentan el tratamiento (Considerandos 12, 58, etc. RGPD), se impone a los operadores el deber de recoger los datos con fines «determinados, explícitos y legítimos», prohibiéndose el tratamiento ulterior de manera incompatible con dichos fines [art. 5.1.b) RGPD]. Se consagra, así, el principio de limitación de la finalidad, que se concreta en el art. 6 RGPD. El tratamiento solo será lícito si se sustentan en el consentimiento del interesado, para un fin concreto o para varios fines, específicamente determinados e individualmente consentidos; si tiene su razón de ser en la ejecución de un contrato en el que el interesado es parte, o porque es imprescindible para la aplicación de medidas precontractuales; porque se impone al operador en cumplimiento de una obligación legal; porque es necesario para la protección de intereses vitales del interesado o de otra persona física; porque es obligatorio para dar cumplimiento o una misión realizada en interés público o en el ejercicio de poderes públicos; o, porque es necesario para la satisfacción de los intereses legítimos

<sup>42</sup> Vid. Dictamen 4/2004 del GT29, de 20 de junio de 2007. En idéntico sentido Resoluciones de la AEPD de 2 de febrero de 2015, de 24 de febrero de 2015 o de 27 de febrero de 2015.

<sup>43</sup> Dictamen 3/2012, del GT29, sobre la evolución de las tecnologías biométricas.

<sup>44</sup> Al respecto, *vid.* Dictamen 02/2013, del GT29, sobre las aplicaciones de los dispositivos inteligentes.

perseguidos por el responsable, siempre que los mismos no entren en colisión con los derechos fundamentales del interesado.

Sobre esta base, queda prohibido el tratamiento de los datos especialmente sensibles, a los que hace referencia el art. 9 RGPD<sup>45</sup>, salvo que concurren algunas de las circunstancias previstas en el párrafo 2.º del precepto, a las que nos remitimos.

Si atendemos a lo analizado hasta ahora en cuanto a la finalidad del tratamiento, es fácil comprender que conforme a lo establecido en el art. 1.2.c) RGPD (art. 2 PLOPD), la norma no resulte de aplicación en aquellos supuestos en los que el tratamiento se lleve a cabo por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas. Es la conocida como «excepción doméstica». Conforme a la misma, el tratamiento de los datos captados por los operadores de aeronaves no pilotadas en actividades estrictamente personales, como puede ser una grabación haciendo deporte o de eventos familiares<sup>46</sup>, etc., estarían excluidos del ámbito de aplicación de la norma, no así, en aquellos casos en los que, por ejemplo, los utilicen para vigilar un determinado espacio, cuando el mismo implique captación, aunque sea parcial, en lugares públicos, que sí estaría sometido a las normas sobre protección de datos<sup>47</sup>.

Como se puede deducir de lo expuesto, y si tenemos en cuenta el exhaustivo régimen jurídico que gira en torno a la protección de los derechos que hemos analizado, es fácilmente comprensible que solo por Ley y, sobre la base de razones o intereses superiores debidamente justificados<sup>48</sup>, puedan establecerse límites a los mismos.

Es indudable, además, que dichas limitaciones solo podrán predicarse de las que hemos calificado como «operaciones públicas», en las que el principio de finalidad y limitación adquiere un papel primordial, de tal forma que dichas

<sup>45</sup> Aquellos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física. Respecto de los cuales se faculta, incluso, a los Estados miembros para establecer condiciones adicionales, *ex art.* 9.5.

<sup>46</sup> Siempre, evidentemente, que no afecte a los derechos de terceros. Lo que se relaciona, íntimamente, con la difusión que pueda darse, por ejemplo en redes sociales, de los datos personales que el operador haya podido obtener, al amparo de la excepción doméstica, en cuyo caso podríamos hablar de una conculcación de las normas sobre protección de datos personales. Precaución ha de tener también el operador, cuando la grabación se exceda a lugares públicos, como pueden ser, por ejemplo, las zonas públicas de una comunidad de propietarios. *Vid.* Resolución de la AEPD de 14 de noviembre de 2016.

<sup>47</sup> *Vid.* C. PAUNER CHULVI, «El uso emergente de drones civiles en España. Estatuto jurídico e imparto en el derecho a la protección de datos», *UNED. Revista de Derecho Político*, núm. 95, enero-abril de 2016, pp. 95 y 96, trayendo a colación la STJUE de 11 de diciembre de 2014, asunto C-212/13, en la que de forma expresa (FJ 35) se indica que «la utilización de un sistema de cámara de vídeo, que da lugar a la obtención de imágenes de personas que luego se almacenan en un dispositivo de grabación continuada, como un disco duro, sistema de videovigilancia instalado por una persona física en su vivienda familiar con el fin de proteger los bienes, la salud y la vida de los propietarios de la vivienda y cuya vigilancia cubre también el espacio público, no constituye un tratamiento de datos efectuado en el ejercicio de actividades exclusivamente personales o domésticas a efectos de la citada disposición de la Directiva». Destacar, también, la información que contiene la «Guía de videovigilancia», elaborada por la AEPD, en <http://www.agpd.es/portalsewebAGPD/canaldocumentacion/publicaciones/common/pdfs/GuiaVideovigilancia2014.pdf>.

<sup>48</sup> Así lo puso de relieve el GT29 en su Opinión 1/2015.

operaciones solo podrán ser llevadas a cabo en los estrictos márgenes de actuación y competencia previstos en la norma que las regule. Hablamos, trayendo a colación las palabras del legislador europeo en los Considerandos 11 y 12 de la DPD2016 de la prevención, investigación, detección o enjuiciamiento de infracciones penales, «incluidas las actuaciones policiales en las que no hay constancia de si un incidente es o no constitutivo de infracción penal». También puede considerarse incluido el ejercicio de la autoridad mediante medidas coercitivas «como es el caso de las actuaciones policiales en manifestaciones, grandes acontecimientos deportivos o disturbios, también en el mantenimiento del orden público». La realización de captaciones y el tratamiento de los datos personales captados, con finalidad distinta a la que señalamos, quedará sometido a las previsiones contenidas en el RGPD.

Hasta que se incorpore la DPD2016, conforme a lo establecido en la LO 4/1997 la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad del Estado<sup>49</sup>, para la grabación de imágenes y sonidos en lugares públicos, abiertos o cerrados, y su posterior tratamiento, solo podrá llevarse a cabo «a fin de contribuir a asegurar la convivencia ciudadana, la erradicación de la violencia y la utilización pacífica de las vías y espacios públicos, así como de prevenir la comisión de delitos, faltas e infracciones relacionados con la seguridad pública» (art. 1).

## **2. Especialidades de la protección de datos en «operaciones privadas» con aeronaves pilotadas por control remoto: examen del Reglamento General de Protección de Datos europeo**

El objetivo del legislador comunitario, no ha sido precisamente, y como es obvio dada su condición de Reglamento General, el establecimiento del marco jurídico específico, que demandamos, para la captación y tratamiento de datos personales en las operaciones con aeronaves pilotadas por control remoto. Consciente de ello, no podemos negar que la aplicación de la norma, prevista para el 28 de mayo de 2018, introducirá importantes mejoras en el régimen general de la protección de datos de carácter personal, de las que como no pudiera ser de otra forma, se beneficiarán los titulares de los datos obtenidos y tratados en el ámbito que analizamos.

Muchos han sido los inconvenientes que, en la materia, se derivaban del régimen anterior contenido en la DPD y en la LOPD (deficiencias en la obligación de información, dificultades para recabar el consentimiento expreso, principios imperantes en materia de calidad de los datos, mecanismos de protección y seguridad de datos y ficheros, etc.), a nuestro estudio de los mismos nos remitimos<sup>50</sup>. Nos proponemos en este trabajo examinar el Texto comunitario con la intención de buscar la solución a los problemas e intentar exponer cuales son las obligaciones que, en materia de protección de datos de carácter personal, se im-

<sup>49</sup> *Vid.*, en cuanto a las funciones que les son propias, LO 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad del Estado y LO 4/2015, de 30 de marzo, de protección de la seguridad ciudadana.

<sup>50</sup> P. MÁRQUEZ LOBILLO, «Incidencia de la aprobación del Reglamento (UE) 2016/679 de 27 de abril de 2016...», *op. cit.*

ponen a los «operadores privados» de aeronaves pilotadas por control remoto, limitándonos a aquellos aspectos que consideramos pueden plantear especialidades y remitiéndonos en los que no al Texto comunitario.

La primera solución o ventaja se encuentra en la armonización legislativa. El hecho de que estemos ante un Reglamento, contribuye a paliar los inconvenientes derivados de las divergencias en la aplicación y ejecución de la Directiva de Protección de datos del año 1995 y garantiza un nivel uniforme y elevado de seguridad y protección, coherente y homogéneo, respetuoso, como de forma expresa se indica, con la idiosincrasia propia de los pueblos europeos, manifestada, por ejemplo, en el reconocimiento de un margen de maniobra a los Estados miembros para determinar las circunstancias relativas a situaciones específicas de tratamiento, «incluida la indicación pormenorizada de las condiciones en las que el tratamiento de datos personales es lícito», o relacionadas con los denominados datos especialmente sensibles (Considerando 10).

En segundo lugar, debe destacarse que el legislador comunitario imponga al responsable del tratamiento la adopción de políticas y medidas internas que cumplan los principios de la protección de datos desde el diseño y por defecto (Considerando 78)<sup>51</sup>, como ya recomendada el GT29 en su Opinión de 2015. El régimen jurídico de este sistema se concreta en el art. 25 de la norma, conforme al cual se impone al responsable del tratamiento, tanto en el momento de determinar los medios de tratamiento como en el del tratamiento mismo (teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas), «la aplicación de medidas técnicas y organizativas apropiadas, como la seudonimización, concebida para aplicar de forma efectiva los principios de protección de datos, o como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados»

Se pretende con ello que, por defecto, solo sean objeto de tratamiento los datos personales necesarios para cada uno de los fines específicos en los que se fundamenta el mismo. Como consecuencia, se impone la obligación, se aplica a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. El objetivo es, en particular, que por defecto los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

Como garantía de cumplimiento de esta obligación el legislador se remite a la posibilidad de utilizar los mecanismos de certificación en materia de protec-

---

<sup>51</sup> F. J. SEMPERE SAMANIEGO, *Comentarios prácticos a la Propuesta de Reglamento...*, op. cit., pp. 284 y ss.; J. VILLARINO MARZO, «La privacidad desde el diseño en la Propuesta de Reglamento Europeo de protección de datos», *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 32, 2013, pp. 45 y ss. Sobre los antecedentes de su implantación e inserción como estándar en el marco jurídico internacional, *vid.* el informe del Grupo de Trabajo Europeo del art. 29, de 1 de diciembre de 2009, «The future of privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data» (02356/09/EN. WP 168), apdos. 44 y ss.; y la Resolución sobre «Privacidad por diseño», adoptada en la 32.ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, Israel, 2010.

ción de datos o los sellos o marcas específicos al respecto, que se contemplan en el art. 42 RGPD<sup>52</sup>. Novedad introducida en el Texto comunitario que, al hilo de la demanda de un régimen jurídico conjunto de la materia que analizamos, en el intervengan junto al poder legislativo como la industria, debe considerarse otra ventaja de la norma que debe ser vista como general<sup>53</sup> y no solo predicable de la garantía de cumplimiento de la privacidad desde el diseño y por defecto.

Analizando los principios en los que ha de sustentarse el tratamiento de datos de carácter personal, enumerados en el art. 5 de la norma, observamos una mayor claridad en su concreción. Se impone la obligación de que los datos sean tratados con licitud, lealtad y transparencia, en relación con el interesado; de forma limitada a la finalidad del mismo, para fines determinados, explícitos y legítimos, sin que sea posible el tratamiento ulterior de manera incompatible con dichos fines<sup>54</sup>; conforme al principio de minimización a lo estrictamente necesario en relación con los fines del tratamiento; con exactitud y si es necesario actualización, adoptándose todas las medidas razonables para suprimir o rectificar sin dilación los datos inexactos; limitando el plazo de conservación de los mismos al tiempo necesario para el cumplimiento de los fines del tratamiento<sup>55</sup>; y aplicando las medidas técnicas y organizativas apropiadas para garantizar la seguridad del fichero, incluida la protección contra el tratamiento no autorizado o ilícito, contra la pérdida, destrucción o daño accidental.

Todo ello, sobre la base del principio de responsabilidad proactiva del operador, *ex art. 5.2*.

El Texto comunitario resulta mucho más clarificador también en orden al establecimiento de las causas o motivaciones que pueden fundamentar el tratamiento de datos (art. 6), que habrá de sustentarse imperativamente en el consentimiento expreso e informado<sup>56</sup> del interesado a tal fin, recayendo sobre el

---

<sup>52</sup> Conforme a lo establecido en el art. 39 PLOPD, la acreditación de las instituciones de certificación a las que se refiere RGPD será llevada a cabo por la Entidad Nacional de Acreditación (ENAC), que comunicará a la Agencia Española de Protección de Datos y a las autoridades de protección de datos de las comunidades autónomas las concesiones, denegaciones o revocaciones de las acreditaciones, así como su motivación.

<sup>53</sup> La importancia de los códigos de conducta y de los sellos de garantía se pone de relieve en los Considerandos 98, 99 y 100 del RGPD. La materialización de su importancia se plasma, por mencionar algunos ejemplos relevantes, en el art. 24.3 del RGPD, cuando prevé que: «La adhesión a códigos de conducta aprobados a tenor del art. 40 o a un mecanismo de certificación aprobado a tenor del art. 42 podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento»; o en el art. 34.8 cuando indica que «El cumplimiento de los códigos de conducta aprobados a que se refiere el art. 40 por los responsables o encargados correspondientes se tendrá debidamente en cuenta al evaluar las repercusiones de las operaciones de tratamiento realizadas por dichos responsables o encargados, en particular a efectos de la evaluación de impacto relativa a la protección de datos». La importancia de la autorregulación se pone de relieve, igualmente, en el PLOPD, art. 38, que prevé que serán aprobados por la Agencia nacional de protección de datos o por la correspondiente Agencia autonómica; serán registrados con accesibilidad por medios electrónicos; y, habrán de ser aprobados conforme al procedimiento que reglamentariamente se establezca.

<sup>54</sup> No considerándose incompatible, en este sentido, conforme al art. 89.1, el tratamiento ulterior con fines de archivo en interés público, investigación científica e histórica o estadística.

<sup>55</sup> Excepción hecha de lo previsto en el art. 89.1 RGPD.

<sup>56</sup> Para que el consentimiento sea informado, el interesado debe conocer como mínimo la identidad del responsable del tratamiento y los fines del tratamiento a los cuales están destinados los datos personales (Considerando 42). El consentimiento además deberá ser libre, estableciendo el legislador el

responsable del fichero la carga de probar la existencia de dicho consentimiento (art. 7 y Considerando 42)<sup>57</sup>.

No encontramos, sin embargo, en las condiciones del consentimiento del art. 7, mecanismos que nos permitan paliar los inconvenientes que en orden a la prestación del mismo manifestó el GT29, salvo que exista alguna relación contractual previa entre el operador y el titular de los datos. El grupo planteó, en relación con el consentimiento libre e informado, la difícil obtención del mismo en las operaciones que analizamos, sobre todo cuando los datos se recaban en zonas públicas. Señalaba que la libertad de consentimiento difícilmente podría darse cuando el sujeto no es libre de entrar y salir en la zona estudiada sin ser objeto de vigilancia; difícilmente será informado, decía, cuando no sabe que está siendo captado, o cuando no se le proporciona información detallada sobre el tratamiento y las condiciones o finalidades del mismo.

Al hilo de lo anterior y, en nuestra opinión, como *conditio sine qua non* para que el consentimiento del interesado cumpla las exigencias del Reglamento, el legislador introduce importantes mejoras en la regulación del deber de información sobre todos los aspectos relacionados con la exactitud de los datos, su captura, almacenamiento, tratamiento, seguridad, responsabilidad y titularidad de los ficheros, ejercicio de los derechos de acceso, rectificación, cancelación, oposición y subsanación, etcétera (arts. 12 y ss.)<sup>58</sup>.

Por la tipología de operaciones susceptibles de efectuarse con las aeronaves que analizamos, por el tamaño de las mismas, por las dificultades que puede entrañar visualizarlas desde tierra, etc., merece mención especial el deber de información contemplado en el art. 14 del Texto comunitario, orientado a que el usuario conozca, todos los elementos de la captación, almacenamiento y tratamiento, y pueda actuar en consecuencia, ejercitando los derechos que contem-

---

derecho del interesado a prestarlo y revocarlo en cualquier momento, sin sufrir perjuicio alguno, debiendo prever el responsable del fichero mecanismos fáciles de revocación. Se prevén, además, especiales medidas en relación con los datos sensibles.

<sup>57</sup> La lectura del precepto, así como los Considerandos 32 y ss. de la norma eliminan cualquier duda en torno a la legitimidad para el tratamiento por parte del responsable sobre la base de un consentimiento presunto. El consentimiento, señala el legislador, «debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada e inequívoca del interesado de aceptar el tratamiento de los datos de carácter personal que le conciernen, como una declaración por escrito, inclusive los medios electrónicos, o una declaración verbal», deberá recaer para todas las actividades realizadas con el mismo o los mismos fines, de tal forma que, en caso de que el tratamiento se fundamente en varios fines distintos, debe darse un consentimiento para todos ellos (Considerando 32). El responsable habrá de proporcionar al interesado un modelo de declaración de consentimiento elaborado con una formulación inteligible y de fácil acceso que emplee un lenguaje claro y sencillo, y que no contenga cláusulas abusivas (Considerando 42).

Al consentimiento expreso se refieren, igualmente, el art. 6 PLOPD, que matiza en la importancia de consentimientos plurales, cuando se realicen tratamientos con varias finalidades; y en que lo puede supeditarse la ejecución de un contrato a que el afectado consienta el tratamiento de los datos, salvo, como resulta lógico, que guarde relación con el mantenimiento, desarrollo y control de la relación contractual.

El art. 7 del PLOPD se ocupa del consentimiento de menores para afirmar que solo puede fundar el tratamiento si el menor tiene más de trece años, salvo que la ley exija la asistencia de los representantes de la patria potestad. En otro caso, será necesario el consentimiento de estos últimos.

<sup>58</sup> Sobre el mismo destacamos una vez más el papel de la AEPD, la Agencia Catalana y la Vasca en la «Guía para el cumplimiento del deber de informar», de 2017, a la que se puede acceder en <https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/modeloclausulainformativa.pdf>.

pla la norma, con posterioridad a la mencionada captación, dado que los datos pueden haber sido recabados sin su consentimiento previo<sup>59</sup>. Sería el supuesto que hemos denominado de captaciones incidentales.

Una buena solución podría ser, en este sentido, la propuesta por la Agencia Europea de Seguridad Aérea que aboga por la creación de una aplicación web en la que se autoinscriban los operadores, mantenida y controlada por las autoridades nacionales de protección de datos. Propone también la instalación de tarjetas (*chips-sim*) en los drones en la que se podría contener toda la información necesaria para garantizar la protección de los datos personales<sup>60</sup>.

En relación con el supuesto de las captaciones incidentales, podría plantear algún inconveniente el concepto de interés legítimo<sup>61</sup> del responsable que puede servir de base al tratamiento *ex art. 14.2.d*), por remisión a los arts. 6.1.f)<sup>62</sup> y 9.2.a)<sup>63</sup>, sobre todo por el debate que en torno al mismo ha surgido en el ámbito de las relaciones contractuales de carácter laboral. El uso de aeronaves pilotadas por control remoto para las labores de prevención y seguridad en las empresas es cada vez mayor, como probable es que en el cumplimiento de dichas funciones se capten incidentalmente, e ilícitamente por ser contrario al principio de finalidad, datos de los trabajadores. Debemos reconocer, no obstante, la importante labor de interpretación jurisprudencial y administrativa que hay detrás del concepto de interés legítimo, que entendemos plenamente aplicable a la norma contenida en el art. 14 RGPD<sup>64</sup>.

<sup>59</sup> Excepción hecha de los supuestos contemplado en el art. 14.5, en los que no será necesario suministrar la información exigida en los apdos. 1 a 4 de la norma. Se trata, en líneas generales, de supuestos en los que la captación tiene fundamentación legal, el interesado ya dispone de la mencionada información, o el suministro de la misma es imposible o supone un esfuerzo desproporcionado para el responsable.

<sup>60</sup> EASA, «Concept of Operations for Drones. A risk based approach to regulation of unmanned aircraft», mayo de 2015.

<sup>61</sup> En el Considerando 49 de la norma el legislador aclara que constituye un interés legítimo el tratamiento de datos personales en la medida estrictamente necesaria y proporcionada para garantizar la seguridad de la red y de la información, es decir la capacidad de una red o de un sistema informático de resistir, en un nivel determinado de confianza, a acontecimientos accidentales o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos personales conservados o transmitidos, y la seguridad de los servicios conexos ofrecidos por, o accesibles a través de, estos sistemas y redes, por parte de autoridades públicas, equipos de respuesta a emergencias informáticas (CERT), equipos de respuesta a incidentes de seguridad informática (CSIRT), proveedores de redes y servicios de comunicaciones electrónicas y proveedores de tecnologías y servicios de seguridad. En lo anterior cabría incluir, por ejemplo, impedir el acceso no autorizado a las redes de comunicaciones electrónicas y la distribución malintencionada de códigos, y frenar ataques de «denegación de servicio» y daños a los sistemas informáticos y de comunicaciones electrónicas.

<sup>62</sup> Conforme a la norma, se considera tratamiento lícito aquel que «es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño».

<sup>63</sup> Relativo al tratamiento de datos considerados especialmente sensibles. En relación con los mismos, la norma amplía la catalogación incluyendo, lo que resulta interesante al objeto de esta investigación, los datos genéticos y biométricos que permitan la identificación o autenticación inequívoca de una persona (Considerando 51), respecto de los cuales se prevé incluso que los Estados miembros puedan mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento (art. 9.4). Estos ya habían sido reconocidos como datos de carácter personal por el Grupo de Trabajo del art. 29 en su *Documento de Trabajo sobre datos genéticos*, de 17 de marzo de 2004 (12178/03/ES, WP91).

<sup>64</sup> Toda esta problemática y el contenido de las resoluciones ha sido analizada por F. J. SEMPERE SAMANIEGO, *Comentarios prácticos a la Propuesta de Reglamento...*, *op. cit.*, pp. 190 y ss., remitiéndonos a los comentarios del autor.

Otro de los inconvenientes acusados en relación con el deber de información que pesa sobre el responsable del tratamiento es la forma de ejercicio del mismo. Cuando se opera con las aeronaves que analizamos en recintos cerrados, el cumplimiento de la obligación resulta, como es evidente, más fácil, pues bastará con el empleo de carteles informativos o con la entrega de folletos o documentos para recabar el consentimiento. Cuando las operaciones se llevan a cabo en lugares abiertos los problemas se agudizan, por lo que entendemos, que el operador deberá recurrir a su página web, comunicarlo a la Agencia de Protección de datos nacional y autonómica, publicarlo por los cauces de las mencionadas Agencias, o recurrir a la utilización de iconos específicos, por mencionar algunas medidas.

Los problemas se agravan en aquellos supuestos en los que la captación de datos no se ha llevado a cabo con el consentimiento previo del titular de los mismos porque, por ejemplo, se han producido de forma incidental, sin que el objetivo principal de la captación fuese la obtención de datos personales.

De la redacción del art. 12 del RGPD puede deducirse, primero, la preocupación del legislador por la materia y segundo la consagración de dos principios fundamentales. El principio de transparencia<sup>65</sup>, que exige que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro; y el principio de libertad de forma en el suministro de la mencionada información, por escrito, por medios electrónicos o por medios iconográficos normalizados<sup>66</sup>.

La imposición a los responsables del tratamiento de la obligación de realizar una evaluación de impacto sobre privacidad<sup>67</sup> ha venido a mitigar, aunque sea de forma parcial, dado que se limita a operaciones de tratamiento arriesgadas<sup>68</sup>, los problemas relacionados con el suministro de información, y a contribuir, además, conforme a lo expuesto en el Considerando 89 del Reglamento, a eliminar

---

<sup>65</sup> Vid. los Estándares Internacionales sobre protección de datos y privacidad, adoptados en la 31 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, Madrid, 2009 (en [http://www.agpd.es/portalwebAGPD/canaldocumentacion/conferencias/common/pdfs/31\\_conferencia\\_internacional/estandares\\_resolucion\\_madrid\\_es.pdf](http://www.agpd.es/portalwebAGPD/canaldocumentacion/conferencias/common/pdfs/31_conferencia_internacional/estandares_resolucion_madrid_es.pdf)).

<sup>66</sup> En relación con los mencionados principios, *vid.* Considerando 58, en el que el legislador se refiere especialmente al suministro de información a través de la web del responsable. De forma acertada, en nuestra opinión, se prevén en el art. 12 los mecanismos para evitar abusos por parte de los interesados en el ejercicio de este derecho.

<sup>67</sup> Para la elaboración de la misma el responsable deberá recabar el asesoramiento del delegado de protección de datos, si ha sido nombrado (art. 35.2), así como la opinión de los interesados o de sus representantes, si es necesario, «sin perjuicio de la protección de intereses públicos o comerciales o de la seguridad de las operaciones de tratamiento» (art. 35.9).

La existencia del delegado de protección de datos, constituye otra importante mejora en el nuevo régimen tuitivo de este derecho fundamental. Nos remitimos a los arts. 37 y ss. del Reglamento por cuanto consideramos que no se presentan especialidades dignas de ser puestas de relieve en las operaciones con aeronaves no pilotadas.

<sup>68</sup> Entendemos que no existe obstáculo legal para que la evaluación de impacto sobre la privacidad se haga, permítasenos el símil, desde el diseño y por defecto, voluntariamente o como consecuencia del cumplimiento de las obligaciones derivadas de la adhesión a un código de conducta, en cuyo caso, conforme al art. 35.8 «se tendrá debidamente en cuenta al evaluar las repercusiones de las operaciones de tratamiento realizadas».

la carga administrativa que supone para el responsable la obligación general de notificar el tratamiento de datos personales<sup>69</sup>.

La evaluación de impacto sobre la privacidad, que habrá de realizarse con carácter previo al tratamiento de los datos<sup>70</sup> y podrá abordar operaciones de tratamiento similares que entrañen riesgos similares, tiene como objetivo paliar los posibles efectos que producen los supuestos de tratamiento que entraña un alto riesgo para los derechos y libertades de las personas, «en particular si utiliza nuevas tecnologías» (art. 35) y ha de centrarse en el análisis del origen, la naturaleza, la particularidad y la gravedad de dicho riesgo (Considerando 84)<sup>71</sup>.

El legislador no establece una lista enunciativa de supuestos en los cuales se impone la obligación de realizar la evaluación de impacto, dado que la determinación de los mismos compete a la autoridad de control en los términos establecidos en los arts. 35.4, 35.5 y 35.6 y con la publicidad exigida en los citados preceptos. Ello no obstante, prevé en el apdo. 3 del art. 35 que la misma es preceptiva, entre otros casos, en supuestos de tratamiento a gran escala<sup>72</sup> de categorías especiales de datos u observación sistemática a gran escala de una zona de acceso público. Operaciones en las que el empleo de aeronaves pilotadas por control remoto resulta de gran utilidad, pensemos, por ejemplo, en el control de fronteras, grabaciones de mítines políticos, manifestaciones, entradas a museos, espectáculos, *selfies* colectivos, etcétera<sup>73</sup>.

Cuando el responsable observe que el tratamiento puede entrañar un alto riesgo para la protección de datos sino se adoptan medidas para mitigarlo, deberá consultar previamente a la autoridad de control, facilitándole la información

<sup>69</sup> La AEPD ha elaborado una Guía para la Evaluación de Impacto en la Protección de los Datos Personales «con el objeto de promover una cultura proactiva de la privacidad, proporcionando un marco de referencia para el ejercicio de ese compromiso responsable que, a la vez, contribuya a fortalecer la protección eficaz de los derechos de las personas». Se encuentra disponible en [https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia\\_EIPD.pdf](https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf).

<sup>70</sup> Debemos tener en cuenta la exención prevista en el art. 35.10 de la norma, para aquellos casos en los que el tratamiento sea consecuencia o tenga su base en el cumplimiento de una obligación legal, nacional o comunitaria, y se haya efectuado una evaluación de impacto general en el contexto de la adopción de dicha norma. Ello, salvo que los Estados miembros consideren lo contrario.

<sup>71</sup> Conforme a lo establecido en el art. 35.7 deberá contener, como mínimo, las siguientes indicaciones: a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento; b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad; c) una evaluación de los riesgos para los derechos y libertades de los interesados, y d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

<sup>72</sup> No podemos olvidar, en este sentido, que en el caso de grabaciones en la vía pública habrá de estarse a lo previsto en la LO 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las fuerzas y cuerpos de seguridad en lugares públicos. *Vid.* de forma detallada, M.ª J. GUERRERO LEBRÓN, C. CUERNO REJADO y P. MÁRQUEZ LOBILLO, «Aeronaves no tripuladas: estado de la legislación para realizar su integración...», *op. cit.*, pp. 102; F. J. SEMPERE SAMANIEGO, *Comentarios prácticos a la Propuesta de Reglamento...*, *op. cit.*, p. 307; T. VÁZQUEZ RUANO, «Implicaciones legales de las aeronaves tripuladas por control remoto en el ámbito comercial...», *op. cit.*

<sup>73</sup> Los supuestos aparecen claramente explicados en los Considerandos 91, 92 y 93 del Reglamento, a los que nos remitimos. *Vid.* M. F. MORSELLLO, «Aspectos jurídicos principales de las aeronaves sin piloto», en J. I. PEINADO GRACIA (dir.) y M.ª C. MAYORGA TOLEDANO (coord.), *Nuevos enfoques del Derecho aeronáutico y espacial*, Madrid, Marcial Pons, 2014, pp. 531 y ss.

que al respecto exige el art. 36 RGPD. La autoridad habrá de pronunciarse, en los plazos que establece la norma, asesorando al responsable en los supuestos, en que este no formule propuestas que identifiquen o mitiguen suficientemente los riesgos<sup>74</sup>.

El legislador comunitario introduce importantes mejoras en los denominados derechos ARCO (acceso, rectificación, cancelación y oposición), propiciando la actuación rápida, «sin dilación indebida», por parte del responsable en la materialización de las solicitudes que formule el interesado en este sentido; y consagrando la posibilidad de ejercicio por medios electrónicos<sup>75</sup>. Se regulan, además, dos nuevos derechos, el de supresión o derecho al olvido (art. 17) y el de portabilidad de datos (art. 28). No procede, porque entendemos que no concurren especialidades dignas de ser puestas de relieve en cuanto a las operaciones con aeronaves pilotadas por control remoto, poner de relieve más que la mejora en cuanto a materialización y ejercicio, y los inconvenientes que de ella se derivan en cuanto imponen nuevas obligaciones al responsable, compensada quizá con la posibilidad de cobrar una tasa que ha de corresponderse con el servicio prestado.

La seguridad de los datos personales constituye otro de los inconvenientes puestos de relieve en la realización de operaciones con aeronaves pilotadas por control remoto, íntimamente relacionado con la vulnerabilidad de los sistemas de transmisión de datos mediante redes inalámbricas, desde la aeronave a la estación de tierra, o desde los distintas aeronaves que conforman un «enjambre de drones».

Debemos reconocer que el legislador ha realizado una importante labor en materia de seguridad, plasmada en el régimen previsto en los arts. 32 y ss. del Reglamento<sup>76</sup>. Las normas imponen a los operadores-responsables del tratamiento un elenco considerable de obligaciones que parten de la exigencia de aplicar medidas técnicas y organizativas apropiadas, tendentes a garantizar la seguridad del tratamiento (seudonimización y cifrado; confidencialidad, integridad, disponibilidad y resiliencia permanente de sistemas y servicios; capacidad para restaurar la disponibilidad y acceso ante incidentes técnicos, etc.). La adhesión a códigos de conducta vuelve a tener un papel fundamental, toda vez que puede servir de fundamento para demostrar el cumplimiento de los requisitos que en materia de seguridad impone el art. 32.

Destaca, igualmente, las obligaciones contenidas en los arts. 33 y 34 del RGPD<sup>77</sup> por las que se impone al responsable la exigencia de comunicar, tanto a la autoridad de control como al interesado, una violación de seguridad de los datos personales, estableciendo el mecanismo para ello, porque, como señala el

---

<sup>74</sup> Para saber si sus propuestas son o no suficientes, el responsable deberá realizar una evaluación de impacto previa «con el fin de valorar la particular gravedad y probabilidad del alto riesgo, teniendo en cuenta la naturaleza, ámbito, contexto y fines del tratamiento y los orígenes del riesgo. Dicha evaluación de impacto debe incluir, en particular, las medidas, garantías y mecanismos previstos para mitigar el riesgo, garantizar la protección de los datos personales y demostrar la conformidad con el presente Reglamento» (Considerando 90 del RGPD).

<sup>75</sup> Vid. arts. 15, 16 y 21 RGPD.

<sup>76</sup> Vid. Considerandos 39, 49, 78 (respecto de la minimización de datos y la seudonimización), 83 (respecto de la aplicación de posibles técnicas de cifrado), etcétera.

<sup>77</sup> Vid. Considerandos 85 y ss. del RGPD.

legislador en el Considerando 85, en caso de que dicha violación se produzca, no nos enfrentamos a un problema baladí, muy al contrario:

«Si no se toman a tiempo medidas adecuadas, las violaciones de la seguridad de los datos personales pueden entrañar daños y perjuicios físicos, materiales o inmateriales para las personas físicas, como pérdida de control sobre sus datos personales o restricción de sus derechos, discriminación, usurpación de identidad, pérdidas financieras, reversión no autorizada de la seudonimización, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, o cualquier otro perjuicio económico o social significativo para la persona física en cuestión».

Es cierto que, los mecanismos expuestos, constituyen una mejora importante en el régimen general tuitivo del derecho fundamental a la protección de datos personales, de la que se beneficiará, sin lugar a dudas, el sujeto cuyos datos hayan sido captados en operaciones con aeronaves pilotadas por control remoto. A pesar de reconocer las ventajas, no debemos dejar de poner de relieve los inconvenientes, relacionados, una vez más, con las especiales características que poseen las aeronaves que analizamos.

El elenco de obligaciones que impone el legislador europeo puede suponer un importante obstáculo a la industria, provocado, quizá, por el hecho de que se imponen en una norma que por su carácter general no tiene en cuenta las especialidades de las captaciones y tratamientos efectuados por estos y con estos vehículos aéreos; o quizá, porque se comete en error de someter todas las aeronaves y todas las operaciones realizadas con ellas al mismo régimen jurídico, sin diferenciación, sin atención al riesgo como exigen las instituciones comunitarias y aquellas que tienen competencias en la protección del tratamiento de datos personales.

Así las cosas, un operador previsor, que en el marco de sus operaciones con aeronaves no pilotada se dedique a la cartografía, a realizar mediciones de terrenos, a comprobar el estado de los cultivos y poder actuar sobre ellos, deberá si quiere evitar sanciones derivadas de una captación de datos incidental, cumplir con todas las exigencias expuestas e, incluso, cuando por la naturaleza de la operación que se esté efectuando puede que no resultar necesario y baste, dado lo improbable de captar datos personales, por ejemplo, con el cumplimiento de las obligaciones administrativas que impone el RD 1036/2017, en aras de que en su caso pueda identificarse al sujeto ante quien ejercitar los derechos ARCO o el derecho al olvido.

Queda mucho camino aún por andar, al menos hasta que el legislador tome conciencia de la necesidad de normas específicas sobre protección de datos personales captados y tratados en «operaciones privadas» realizadas con aeronaves pilotadas por control remoto.

### **3. Especialidades de la protección de datos en «operaciones públicas» con aeronaves pilotadas por control remoto: régimen actual y perspectivas de futuro**

El GT29 realizaba una afirmación que consideramos digna de transcripción literal, íntimamente vinculada al uso de aeronaves no pilotadas en las opera-

ciones que hemos calificado como públicas: «*This will result in an increased feeling of being under surveillance and a subsequent possible decrease in the legitimate exercise of civil liberties and rights, best known as “chilling effect”*». Sobre esta base nos proponemos analizar el régimen jurídico actual y mencionar, brevemente, las mejoras que se introducirán con la incorporación a nuestro ordenamiento de la DPD2016.

### A) Régimen jurídico actual

La inclusión de los RPAS en el ámbito de aplicación de la LO 4/1997, y para la finalidad estrictamente prevista en la misma, analizada en el lugar oportuno de este trabajo, se fundamenta en la consagración del principio de equivalencia funcional, en el apdo. 2 del art. 1.

Conforme a lo previsto en la norma, la captación, reproducción y tratamiento de datos personales, en los términos previstos en esta Ley<sup>78</sup>, no se considera intromisión ilegítima en el derecho al honor, a la intimidad personal y familiar y a la propia imagen (art. 2).

Habrán de observarse las normas contenidas en la Ley de Enjuiciamiento Criminal (autorización judicial salvo que medie consentimiento expreso del titular de los derechos)<sup>79</sup> en aquellos casos en los que la aeronave vaya a ser utilizada para tomar imágenes y sonidos en el interior de las viviendas, y sus vestíbulos (art. 6.5)<sup>80</sup>; o en lugares públicos en los que se afecte de forma directa y grave a la intimidad de las personas, prohibiéndose expresamente la grabación de conversaciones de naturaleza estrictamente privada (art. 6.5). Se impone, en estos casos, la obligación del «operador público-responsable del tratamiento», de destruir de forma inmediata los datos obtenidos incidentalmente.

---

<sup>78</sup> Queremos resaltar la concreción legislativa, en el sentido de que para que no se considere que existe intromisión ilegítima es necesario el cumplimiento de las previsiones legales en cuanto a la instalación de los dispositivos que contempla. En otro caso, es decir, cuando la instalación no se acomode a dichas previsiones estaremos en presencia de una intromisión ilegítima sometida a la LO 1/1982, de 5 de mayo, con las salvedades que hemos expuesto anteriormente.

<sup>79</sup> Arts. 588.bis.a) y ss.

<sup>80</sup> De forma detallada F. BUENO MATA, «Drones, virus espía y agentes encubiertos en la Red: comentarios a las nuevas medidas de investigación tecnológica en la normativa procesal española», Ponencia presentada al XIX Congreso Iberoamericano de Derecho e Informática, Medellín, agosto de 2015, disponible en <http://fiadi.org/wp-content/uploads/2015/08/Federico-Bueno-de-Mata.pdf>; M.ª N. DE LA SERNA BILBAO, «Seguridad ciudadana y los sistemas de videovigilancia. Límites, garantías y regulación», *IUSTA*, núm. 45, julio-diciembre de 2016, pp. 129 y ss.

Nos hemos permitido utilizar la expresión domicilio de forma consciente, dada la interpretación amplia que de su concepto ha hecho nuestro Tribunal Supremo, destacando la Sentencia de 24 de enero de 2012 (el domicilio social), y ATS de 14 de febrero de 2013 (un camarote). Por todos, P. BENAVIDES VELASCO, *El domicilio de las sociedades mercantiles de capital*, Granada, Comares, 2004.

Recientemente, en su Sentencia de 20 de abril de 2016, con alusión específica al uso de drones, el Tribunal Supremo ha afirmado que «protección constitucional frente a la incursión en un domicilio debe abarcar, ahora más que nunca, tanto la entrada física del intruso como la intromisión virtual. La revolución tecnológica ofrece sofisticados instrumentos de intrusión que obligan a una interpretación funcional del art. 18.2 CE. La existencia de drones, cuya tripulación a distancia permite una ilimitada capacidad de intromisión en recintos domiciliarios abiertos es solo uno de los múltiples ejemplos inimaginables».

Conforme a lo previsto en el art. 5 de la norma, que entendemos es la que resulta aplicable a las RPAS por su carácter móvil, las mismas podrán utilizarse en las vías y lugares públicos donde se haya autorizado la instalación de videocámaras fijas (arts. 3 y 4)<sup>81</sup>, para que simultáneamente con ellas, contribuyan al mejor cumplimiento de los fines previstos en la norma, «quedando, en todo caso, supeditada la toma, que ha de ser conjunta, de imagen y sonido, a la concurrencia de un peligro concreto y demás requisitos exigidos en el artículo 6»; o, en otros lugares públicos, previa autorización del máximo responsable provincial de las Fuerzas y Cuerpos de Seguridad<sup>82</sup>, «quien atenderá a la naturaleza de los eventuales hechos susceptibles de filmación, adecuando la utilización del medio a los principios previstos en el artículo 6».

La utilización de RPAS se condiciona al cumplimiento del principio de proporcionalidad (art. 6), en su doble vertiente de idoneidad<sup>83</sup> e intervención mínima<sup>84</sup>. Exigirá, por otro lado, la existencia de un peligro concreto (art. 6.4).

Se consagra en el art. 7 aspectos procedimentales relativos al procedimiento de transferencia de datos a los órganos competentes en los supuestos en los que de la grabación se capte la comisión de hechos que pueden constituir infracción penal o administrativa.

Las grabaciones se destruirán en el plazo máximo de un mes desde su captación, salvo que estén relacionadas con infracciones penales o administrativas graves o muy graves en materia de seguridad pública, con una investigación policial en curso o con un procedimiento judicial o administrativo abierto (art. 8).

El art. 9, en relación con los derechos de los interesados, plantea algún inconveniente que queremos mencionar. Respecto del derecho de información, la norma se refiere, exclusivamente, a la existencia de videocámaras fijas, sin alusión a las móviles y, en consecuencia, sin contemplar los RPAS. Lo que excluye la posibilidad no solo de que el interesado sea informado de la existencia de los mismos y del uso o finalidad con el que se están utilizando, sino de que el mismo pueda ejercer los derechos de acceso y cancelación de las grabaciones que, aunque de forma limitada y fácilmente excepcionable, contempla la norma de 1997 (art. 9.2).

<sup>81</sup> Respecto de la Comisión autorizante y la composición de la misma, así como de los criterios que han de regir la concesión de la autorización, conforme al principio de proporcionalidad (asegurar la protección de los edificios e instalaciones públicas y de sus accesos; salvaguardar las instalaciones útiles para la defensa nacional; constatar infracciones a la seguridad ciudadana, y prevenir la causación de daños a las personas y bienes).

<sup>82</sup> Quien deberá poner en conocimiento de la Comisión del art. 3 la resolución autorizando el uso, en el plazo previsto en el apdo. 5 del art. 5, salvo en casos excepcionales de máxima urgencia o de imposibilidad de obtener a tiempo la autorización, en cuyo caso habrá de darse cuenta, en el plazo de setenta y dos horas, mediante un informe motivado, al máximo responsable provincial de las Fuerzas y Cuerpos de Seguridad y a la Comisión. Si la Comisión emite informe negativo, la autoridad encargada de la custodia de la grabación procederá a su destrucción inmediata.

<sup>83</sup> Conforme a la cual, *ex art. 6.2*, solo podrá emplearse la videocámara cuando resulte adecuado, en una situación concreta, para el mantenimiento de la seguridad ciudadana, de conformidad con lo dispuesto en la norma.

<sup>84</sup> Que exige, *ex art. 6.3*, la ponderación, en cada caso, entre la finalidad pretendida y la posible afectación por la utilización de la videocámara al derecho al honor, a la propia imagen y a la intimidad de las personas.

### *B) La incorporación a nuestro ordenamiento de la DPD2016*

Las mejoras que, en orden al tratamiento de datos personales captados en «operaciones públicas» con aeronaves pilotadas por control remoto se van a derivar de la incorporación de la DPD2016 son indudables, en primer lugar, quizá porque no se establecen diferenciaciones entre dispositivos fijos o móviles de captación y tratamiento de datos. En segundo lugar porque, salvando las distancias que impone la finalidad del tratamiento y el interés público que en la misma subyace, es parangonable con el previsto en el RGPD<sup>85</sup>, lo que sin duda contribuirá a eliminar arbitrariedades y a lograr una mayor protección de los derechos de los ciudadanos.

La afirmación con la que encabezamos este epígrafe se refuerza en el examen de su articulado. Por empezar desde el principio, frente al mero respaldo en una norma y un interés público, que tenemos en la actualidad, se imponen en los arts. 4 y ss. de la DPD2016, principios y obligaciones relacionados con el tratamiento, en orden a conseguir que el mismo sea lícito y leal; determinado, explícito y legítimo; adecuado, pertinente y no excesivo; exactos y, si es necesario, actualizados; por el tiempo estrictamente necesario<sup>86</sup>; garantizando su seguridad; diferenciando a los interesados (presuntos culpables, condenados, víctimas, terceras partes); distinguiendo, en la medida de lo posible, los datos personales basados en hechos de aquellos que se sustentan en apreciaciones personales; controlando la calidad de los datos que se transmiten, de tal forma que no sean inexactos o estén incompletos; imponiendo la limitación del tratamiento a los estrictos fines de la norma; limitando el tratamiento de datos especialmente sensibles.

Mención especial merece, porque así lo reclamó el GT29 a fin de evitar la elaboración de perfiles que puedan producir efectos negativos para el interesado o le afectan significativamente, el contenido del art. 11. La norma prohíbe, salvo autorización legal y garantía de medidas adecuadas de salvaguarda de los derechos y libertades de los interesados, la adopción de decisiones fundadas únicamente en el tratamiento automatizado de los datos, sin tomar en consideración las categorías especiales de personas del art. 10. Destaca, en este sentido, la consagración del derecho del ciudadano a obtener, al menos, la intervención humana por parte del responsable del tratamiento<sup>87</sup> y la prohibición de elaborar perfiles que dé lugar a una discriminación de las personas físicas basándose en la categoría especiales de datos del art. 10.

---

<sup>85</sup> Nos remitimos a lo expuesto en relación con el mismo. Así la obligación de protección de los datos desde el diseño y por defecto (art. 20); la evaluación de impacto relativa a la protección de datos (art. 27); los importantes mecanismos para garantizar la seguridad del tratamiento (arts. 29 y ss.); el delegado de protección de datos (arts. 32 y ss.); las exhaustivas normas en orden a la transferencia de datos (arts. 35 y ss.)

<sup>86</sup> Imponiendo a los Estados miembros la obligación de que se fijen plazos apropiados para la supresión de los datos y de que se revise periódicamente la necesidad de conservación de los mismos (art. 5).

<sup>87</sup> Se nos viene a la mente la reciente Sentencia del Juzgado de lo Contencioso administrativo núm. 6 de Madrid, de mayo de 2017, en la que se ha anulado una sanción de tráfico entendiendo que no se puede sancionar al titular del vehículo en los supuestos en los que no se identifica al conductor, con imágenes grabadas desde el helicóptero. Fallo que bien podría extrapolarse al empleo de una aeronave pilotada por control remoto.

Se regula también, de forma mucho más detallada, el registro de todas las categorías de actividades de tratamiento, al que simplemente aludía el art. 22 LOPD, con mención expresa de su contenido (art. 24).

Se prevé la obligación del responsable o del encargado de consultar con la autoridad de control antes de proceder al tratamiento de datos personales que vayan a formar parte de un nuevo fichero, *ex art. 28.1.b*), por el mero hecho de usar tecnologías, siempre que pueda constituir un alto riesgo para los derechos y libertades de los interesados<sup>88</sup>.

Analizando los aspectos que nos conciernen de los derechos de los interesados, debemos partir de la consagración de un exhaustivo, claro y conciso derecho de información (art. 12), cuyo contenido se consagra en el art. 13 de la norma<sup>89</sup>, por la vía de la exigencia de puesta a disposición u obligación de proporcionarla, por cualquier medio adecuado, incluido los electrónicos.

Nos preocupa, el modo de adecuar el cumplimiento de dicha exigencia a la aeronave pilotada por control remoto, aspecto sobre el que entendemos debería haberse realizado un pronunciamiento expreso en el RD de 2017. Habremos de contentarnos, en este sentido, con la Guía elaborada por la AEPD, la Agencia Catalana y la Vasca, pues aunque la misma se refiere al RGPD, el contenido del deber (excepción hecha de sus salvedades) es sustancialmente idéntico<sup>90</sup>.

Como nos preocupa que no se hayan fijado ni esperamos que se fijen, cuales son las medidas técnicas y organizativas adecuadas para garantizar y estar en condiciones de demostrar que el tratamiento se lleva a cabo de conformidad con lo previsto en la DPD2016 (*ex art. 19*).

En relación con el resto de los derechos (acceso y limitaciones de acceso, de los arts. 14 y 15; rectificación y supresión, art. 16); la trasferencia de datos (arts. 35 y ss.) o las exigencias en orden a la fijación del régimen jurídico de la autoridad de control (arts. 41 y ss.) nos remitimos al contenido de la norma por no encontrar especialidades dignas de ser puestas de relieve en el ámbito que analizamos.

---

<sup>88</sup> Obligación que, en el ámbito de las operaciones que analizados, bien podría exigirse en los supuestos, por ejemplo, de control y vigilancia de manifestaciones, espectáculos, etc., con aeronaves pilotadas por control remoto.

<sup>89</sup> Respecto de las excepciones al mismo, *vid.* art. 13.3, íntimamente relacionadas con la salvaguarda del interés público, la seguridad nacional, y la protección de los derechos y libertades de otras personas.

<sup>90</sup> *Vid. supra.*