FECHA: 13/03/2019

TÍTULO: **DRONES vs. PRIVACIDAD DE DATOS EN LA ERA DIGITAL (*)**

Autor/a: Dra. PILAR DOPAZO FRAGUÍO. Profesora de Derecho Administrativo.
Universidad Complutense de Madrid (UCM)

Sumario

1. LA PROTECCIÓN DE DATOS EN LA ERA DIGITAL: UNA CUESTIÓN DE INTERÉS PÚBLICO.

Los datos son hoy un preciado valor ligado a la persona, digno de especial protección, por ser un bien jurídico altamente sensible, vinculado con el derecho a la privacidad del individuo; asimismo, en el presente, también se configura como un valioso activo, que en orden a su consideración económica -o aplicación comercial- adquiere un interés cada vez mayor. En este sentido, cabe observar el potencial que ofrece dicho activo, en especial para algunos operadores, por lo que el disponer de cierto tipo de información relativa a las personas puede constituir, *per se*, un objetivo estratégico, siendo así ya identificado por distintos sectores. Esto es, en nuestros días, los datos se convierten en una apreciada fuente o recurso, y, en consecuencia, se deberá incrementar su tutela frente a posibles amenazas (v.gr., prácticas de captación, uso o tratamiento no autorizado, de forma expresa, por el titular de los datos). Desde esta perspectiva, cabe advertir sobre la *vis atractiva* que pueden ofrecer los datos personales, ya que el disponer de dicho activo implicaría contar con

* **(*)** Estudio realizado en el marco del proyecto de investigación titulado "El régimen jurídico-público de los drones". Ref.: DER2017-87981-P. - 2018-2020. Proyecto de I+D+i (Conv. 2017. MEIC, Programa Estatal de Investigación, Desarrollo e Innovación orientada a los Retos de la Sociedad).

un elemento clave a la hora de trazar y desarrollar las nuevas estrategias de negocio en el ámbito del comercio digital. Sin duda, lo mencionado incrementa los posibles riesgos que afectarían a la privacidad, interpretada como bien intangible necesariamente vinculado con el derecho fundamental a la protección de datos; siendo por ello digno de especial protección jurídica. En consecuencia, cabe insistir en el deber de garantizar eficaces instrumentos de tutela, conforme a lo previsto por nuestro Ordenamiento vigente, que permitan salvaguardar este preciado binomio "datos y privacidad", objeto del reconocido derecho fundamental a la protección de datos, frente a eventuales prácticas ilícitas, abusivas o no autorizadas.

Lo expresado cobra aún mayor importancia, en nuestros días, ante la evidente proyección de nuevas herramientas y estructuras digitales, ligadas el creciente uso de medios tecnológicos, y, con ello, la generación de modelos de contratación electrónicos. Estas nuevas prácticas surgen de forma progresiva en el tráfico jurídico, y además, -cabe inferir-, con la pretensión de posicionarse, de forma progresiva, frente a las fórmulas operativas/contractuales tradicionales. Sirva de ejemplo, en este sentido, la tendencia observada hacia una posible virtualización de relaciones jurídicas, con base al empleo de contractos atípicos, con objeto de su instrumentalización en los actuales entornos digitales u operativos a través de la Red (o redes). Ello, si bien facilita vías eficaces para el emprendimiento de actividades y prestación de distintos servicios (públicos y privados), -sobre todo por la celeridad que posibilitan-, sin embargo no siempre son seguras[1]. De este modo, en el presente, no se puede ignorar el cambio disruptivo que supone el desarrollo de las TIC, así como de las diversas innovaciones tecnológicas generadas en torno a ellas; lo que influye en todos los órdenes (cultural, social, económico y financiero)[2]. Y, por ende, son significativos los desafíos jurídicos que aún plantean; máxime si consideramos la evidente proyección europea e internacional que acompaña a este tipo de fenómenos emergentes, ligados al uso extensivo de TIC[3], como acontece en el caso del empleo de drones.

En efecto, lo cierto es que, en este contexto dinámico, surgen -de forma paralela- distintos fenómenos, motivados por una mayor accesibilidad a las herramientas tecnológicas hoy disponibles (v.gr., dispositivos, equipos o aparatos relacionados con las tecnologías de la información y la comunicación, TIC); y, entre otros, cabe destacar, -como clara tendencia en auge-, el creciente interés por uso civil o recreativo de drones, aeronaves no tripuladas y que actúan por control remoto, permitiendo la captación de información. Esta práctica a su vez está en plena expansión comercial, y, por tanto, puede ser calificada como un fenómeno actual, cuyo estudio jurídico resulta relevante por los posibles impactos que genera (o pudiera implicar). Desde este

[1] Fruto de lo mencionado, surgen relaciones jurídicas "electrónicas o digitales", que con celeridad abren el paso" al desarrollo de la innovación en procesos y modelos de emprendimiento, así como vículos contractuales o colaborativos (si bien, algunos de los cuales han de ser calificados como atípicos, por aún no disponer de tipificación normativa o base regulatoria).

[2] Al respecto de este cambio, vid., trabajos AA.VV., en "El Cambio Digital en la Economía. Un proceso disruptive". (Ministerio de Economía, Industria y Competitividad) Revista ICE, *Información Comercial Española* nº. 897, julio-agosto, 2017.

[3] A modo de ejemplo, obsérvese el desarrollo de las denominadas "criptomonedas" (*cryptocurrencies*), el *bitcoin* o BTC, entre otras, y su utilización como fórmulas alternativas de financiación estas monedas "virtuales", así como la tecnología en la que se sustentan, *blockchain*. Tal y como advierte, Domingo CARBAJO VASCO, "la realidad social y económica no esté muchas veces recogida de forma precisa o literal por el Derecho, por las normas jurídicas, pues la construcción de la disposición normativa es retardataria, posterior a los hechos y a la realidad social, como ha sucedido siempre en múltiples contratos mercantiles (arrendamiento financiero o franquicia, por poner dos ejemplos) y en muchos aspectos sociales (la convivencia de hecho entre parejas o la formación de lo que se conoce como "nuevas fórmulas familiares") que existían mucho antes de que el Ordenamiento jurídico las incorporase, definiese, diese forma y regulase" (p. 9). CARBAJO VASCO, D., "El desarrollo de las criptomonedas y su tributación. Cuestiones y respuestas.". *Blockchein Intelligence*. BI Blockchein Law Institute. Serie Doctrinal nº 1. Madrid, junio de 2018. pp. 3-44.

enfoque, en particular, esta cuestión es de interés jurídico público, observando la naturaleza de los efectos que el empleo civil de drones puede conllevar para la ciudadanía; y, de forma específica, en relación con la eventual vulneración de derechos y libertades fundamentales. Lo advertido adquiere especial relieve, si consideramos la posible incidencia de estos artefactos en el ámbito que comprende la privacidad de las personas, y sobre todo estimando el valor que identifica a los datos personales en nuestros días (tal y como ha sido expuesto en párrafos precedentes). Al respecto, conviene tener presente las propiedades que caracterizan a este valioso intangible; y, de este modo, los datos relativos a una persona física son patrimonio privativo de cada individuo, al que como (único) titular de los mismos corresponde decidir sobre su empleo o disposición. Por tanto, el binomio privacidad y datos constituye un "bien jurídico cualificado", objeto de especial protección con base al propio reconocimiento del derecho fundamental a la protección de datos consagrado por el Ordenamiento europeo y nacional vigente.

Como toda tecnología, el empleo de drones aporta ventajas, en tanto su aplicación es destinada a cumplir finalidades concretas, -v.gr., servicios públicos o de interés colectivo-, pero también su utilidad por particulares o empresas produce eventuales efectos adversos (caso de acciones negligentes o incluso prácticas ilícitas). En consecuencia, ha de tenerse muy en cuenta el deber de prevención y tutela pública que ha de concurrir al respecto, en aras de asegurar el adecuado cumplimiento de la legislación vigente, tanto en lo relativo a la normativa aplicable al uso civil de drones, como aquella relativa a la protección de datos. Lo que a su vez conlleva reforzar las oportunas medidas de disciplina y control, por parte de las autoridades competentes, europeas y nacionales.

En este sentido, cabe significar la positiva evolución de la normativa europea y nacional,–tal y como se detalla en este estudio–, que establece determinados requerimientos para el empleo de drones, así como la previa acreditación de determinadas garantías por lo que respecta al cumplimiento de la legislación actual en materia de protección de datos. Lo cual, conlleva deberes concretos para los operadores, obligados a seguir determinados sistemas de gestión y adoptar medidas específicas de tratamiento, prevención de riesgos y ciberseguridad. En su defecto, asumirían las responsabilidades derivadas de los daños y perjuicios causados, amén de enfrentarse a las correspondientes sanciones administrativas (cfr., régimen jurídico previsto por el vigente *Reglamento general de protección de datos* (RGPD, 2016)[4].

Considerando la relevancia de esta cuestión de actualidad jurídica, el presente estudio se centra en el análisis del "fenómeno de los drones" en relación con su (posible) impacto sobre la privacidad y el derecho a la protección de datos, y a dicho interés, es objeto de especial examen la vigente legislación europea y nacional aplicable en materia de protección de datos. Con ello, se pretenden destacar cuáles son las principales aportaciones de la reciente regulación europea y española promulgada en esta materia, así como detallar el conjunto de requerimientos exigidos a los operadores responsables, en virtud de dicha normativa.

2. EL FENÓMENO DE LOS DRONES Y TRATAMIENTO JURÍDICO.

En la actualidad, se observa un uso creciente y amplio de drones, para fines civiles o recreativos, más allá de su empleo original para finalidades militares, defensa y seguridad, claramente de interés general y con base a servicios de carácter público. Por tanto, advirtiendo que la proyección actual de estas aeronaves también se orienta a otras utilidades o aplicaciones, –tal y como ya aconteciera en el pasado con otras innovaciones tecnológicas, v.gr., internet, telefonía móvil, robótica, etc.–,

[4] Reglamento (UE) 2016/679, del Parlamento europeo y de Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. DOUE L 119/1, de 4.5.2016.

resulta conveniente reflexionar sobre los riesgos que ello conlleva (sobre todo, caso de prácticas realizadas por personas no cualificadas).

De este modo, no puede ignorarse que el empleo civil de drones puede incidir en derechos fundamentales, tales como el derecho reconocido a la protección de datos, que es un derecho fundamental, personalísimo, y como tal, los datos se configuran como un bien ligado a la personalidad del individuo, siendo intransferibles sin el consentimiento *expreso* de su titular. Por ende, la tutela pública brindada por el Ordenamiento a este derecho es una cuestión nuclear, ya que solo mediante una regulación vinculante, uniforme y común, que resulte eficaz en la práctica, podrá asegurarse una disciplina satisfactoria; esto es, capacitada para prevenir y, en su defecto, enfrentar cualquier tipo de práctica que pudiera suponer la efectiva vulneración de este derecho. Pues, además de la legislación dictada sobre el tráfico de los drones, -y con el fin de asegurar que su navegación sea con "rumbo cierto, lícito y seguro"-, también debe tenerse en cuenta el cumplimiento de la regulación específicamente aplicable en materia de protección de datos; por cuanto, hay que reconocer los riesgos que supone el uso de drones, v.gr., efectos adversos sobre las personas, daños efectivos, físicos y/o morales, que a su vez pudieran ser directos o indirectos, o producidos a largo plazo, y que con todo implicarían altos costes (en especial, ante supuestos en los que no se disponga de suficientes garantías o coberturas financieras). Asimismo, nótese como dificultad añadida a lo mencionado, que en ciertos casos pudiera ser difícil la identificación de los responsables, o no ser viable probar el agente causante de la lesión sufrida en la privacidad, por ejemplo, mediante el uso de drones que captaron determinada información o imágenes de forma oculta o no autorizada. Además, en el tratamiento de datos, se sabe, pueden intervenir varios sujetos u operadores, que no siempre pudiera ser posible concretar (ya que cada uno podrá encargarse de distintas acciones, registro, destino o aplicación final de los datos obtenidos).

Con todo, digno es destacar el avance regulatorio que en materia de protección de datos supone el actual *Reglamento europeo general de protección de datos* (RGPD); y conforme al mismo, en España, la promulgación de la *Ley Orgánica 3/2018, de Protección de Datos y Garantía de los derechos digitales*, de 5 de diciembre (en adelante, LOPDyGDD)[5].

2.1. **Consideraciones previas**.

En primer lugar, conviene precisar la noción de dron o drones, bajo esta terminología[6] se hace referencia al "concepto de aeronave sin piloto o, en términos actuales, vehículos aéreos no tripulados o UAVs" («Unmanned Aerial Vehicle»). Tal y como ha sido interpretado por la comunidad internacional, se trata de aeronaves que vuelan sin piloto/s a bordo, y que son controladas mediante equipos de control remoto, -aeronaves pilotadas por control remoto-; o bien, también cabe su previa programación, tranzado su rumbo, por lo que navegarían de forma

[5] BOE núm. 294, de 6 de diciembre de 2018.

[6] Con carácter general, se emplea el término "dron" o "drones", que procede del vocablo inglés, para referirse a "vehículos aéreos no tripulados", y conforme a distintas siglas, como son UAV (Unnmanned Aerial Vehicle), UA (Unmanned Aircraft), UAS (Unmanned Aerial System), RPA (Remotely Piloted Aircraft) o RPAS (Remotely Piloted Aircraft System). No obstante, cabe precisar que existen distintas modalidades. En particular, bajo el término genérico de "dron /drones" se hace referencia a los aparatos UAV o UA, que se trata de vehículos aéreos no tripulados; en cambio cuando se usa el acrónimo RPA, también dicho vehículo aéreo no tripulado reúne otras propiedades, como son la posibilidad de su autonomía más su pilotaje o control remoto. Por último, también la utilización de UAVS y RPAS aluden a sistemas integrados, más complejos, que comprenden sistemas de control, entre otras posibilidades. Con respecto al concepto de "Dron", vid., SARRIÓN ESTEVE, Joaquín, "El régimen jurídico de la utilización de drones en España", ponencia en Seminari de la Facultat de Dret de València, 25 de Mayo de 2016. Working paper disponible en: https://www.uv.es/seminaridret/sesiones2016/drones/ponenciaSarrion2016 (Fecha última consulta: 23/02/2018). Y, con todo detalle, consultar la obra de GONZÁLEZ BOTIJA, Fernando, *Los drones y el Derecho de la Unión Europea. Reglamento (UE) nº 2018/1139 y propuestas de EASA*. Atelier, Barcelona 2018 (pp. 29-36).

autónoma, -aeronaves autónomas- siendo así conceptuadas por la Organización Internacional de Aviación Civil (OACI)[7].

Sin duda, el uso de este tipo de herramientas destinado a cumplir determinados fines justificados, presenta funcionalidades positivas en interés colectivo, como son aquellas utilidades ligadas a la seguridad, vigilancia y otros servicios públicos. Ello aporta ventajas, pero, por otra parte, también conviene observar que hoy su distribución comercial es cada vez es más amplia, facilitando otros empleos privativos, o para usos meramente recreativos, etc.. Lo que no siempre presupone disponer de la formación técnica necesaria. En este sentido, ya son varios los incidentes producidos, lo que ha provocado lógica preocupación ante el uso civil de drones[8].

Tal y como ha sido expuesto (*supra*), la privacidad de las personas es un valor que puede ser conculcado con facilidad por este tipo de dispositivos, al igual que ya sucede con otras tecnologías inteligentes, implementadas vía sistemas digitales ligados a equipos robóticos, con mayor o menor grado de complejidad o desarrollo. Ello ilustra sobre la necesidad de identificar y prevenir el riesgo que existe ante posibles conductas negligentes, o, incluso, prácticas ilícitas. Por cuanto, al respecto, debe recordarse que, en todo caso y conforme dicta la legislación actual, el titular de los datos es el único que puede decidir y disponer sobre el uso de sus datos; y, en consecuencia, le asiste la facultar de ejercer su derecho de acceso y obtención de información, (para conocer quién y con qué finalidad se recaban sus datos, tipología de datos, y acerca de cuál es el tratamiento dado y destino de los mismos). La legislación vigente en materia de datos (RGPD(es clara en este sentido, exigiendo que para cualquier tratamiento de datos es preciso disponer de la previa autorización *expresa* de su titular. Ergo, en su defecto, cabe interpretar que todo uso no autorizado resultaría ilícito; de igual modo cuando no se cumpla con los deberes dictados en lo relativo a las acciones de tratamiento que corresponden a los sujetos responsables y encargados del mismo, que, asimismo deben acreditar disponer de adecuados sistemas de seguridad frente a cualquier amenaza o eventos adversos, incluidos posible ciberataques (conforme se expone, *infra*).

2.2. Marco normativo.

En sentido amplio, un dron es un tipo de vehículo aéreo, conforme señala la Organización de la Aviación Civil Internacional (OACI)[9], *"Sistema de aeronave pilotada a distancia",* y, como tal, se configura como un *"Conjunto de elementos configurables integrado por una aeronave pilotada a distancia, sus estaciones de piloto remoto conexas, los necesarios enlaces de mando y control y cualquier otro elemento de sistema que pueda requerirse en cualquier punto durante la operación de vuelo*" [10]. En este mismo sentido, la Ley de

[7] Cfr., Artículo 5. *Definiciones.* Real Decreto 1036/2017, de 15 de diciembre, por el que se regula la utilización civil de las aeronaves pilotadas por control remoto, y se modifican el Real Decreto 552/2014, de 27 de junio, por el que se desarrolla el Reglamento del aire y disposiciones operativas comunes para los servicios y procedimientos de navegación aérea y el Real Decreto 57/2002, de 18 de enero, por el que se aprueba el Reglamento de Circulación Aérea. (BOE núm. 316, de 29 de diciembre de 2017).

[8] Por ejemplo, entre otros sucesos, hay que recordar el incidente con drones que provocó la cancelación de 1.000 vuelos en el aeropuerto de Gatwick, en Londres. Fuente informativa: EFE. "¿Es posible acabar con la amenaza de los drones en los aeropuertos?. *www.expansion.com › Economía Digital › Innovación-*. Fecha: 17 enero 2019. En: http://www.expansion.com/economia-digital/innovacion/2019/01/17/5c3daa1fe2704ea2a88b4575.html

[9]Cf., OACI (2011), Sistemas de aeronaves no tripuladas (UAS), Circular 328, disponible en: https://www.icao.int/Meetings/UAS/Documents/Circular%20328_es.pdf; y, vid., https://noticias.canalrcn.com/tecnologia-tecnologia/asociacion-transporte-aereo-internacional-dice-los-drones-son-un-peligro

[10] Conforme al diccionario de la Real Academia Española (RAE): "Dron, Del ingl. drone. 1. m. Aeronave no tripulada". Dron, (en plural "drones"), vocablo que es utilizado para hacer referencia a distintos tipos de aeronaves no tripuladas, y que procede del término inglés "drone", cuyo significado original es zángano o abeja macho, por lo que se emplea esta

navegación aérea española, Ley 48/1960, de 21 de julio, artículos 11 y 150, texto actualizado mediante la Ley 18/2014, de 15 de octubre, de medidas urgentes para crecimiento, la competitividad y la eficiencia, y considerando el previo texto del Real Decreto Ley 8/2014, de 4 de julio, incorpora dentro de la noción de "aeronave" a este tipo de vehículos aéreos, cuando dice, *"b) Cualquier máquina pilotada por control remoto que pueda sustentarse en la atmósfera por reacciones del aire que no sean las reacciones del mismo contra la superficie de la tierra"*. Conforme a la definición precitada (OACI)[11], existen múltiples modalidades o categorías de drones, con base a las "capacidades" y utilidades previstas por la tecnología disponible. Este dispositivo móvil o vehículo aéreo puede ir equipado con sistemas de obtención y/o procesamiento de datos, imágenes u otro tipo de información (por lo que, por lo común, permite el procesamiento de datos). Así, por ejemplo, integra desde sistemas de captación de imágenes, sistemas de localización y seguimiento, mecanismos complejos de grabación y de detección (sensores ópticos o electrónicos, medición de temperaturas, infrarrojos, detectores de partículas, contaminación o emisiones, entre otros posible, etc.), u otros medios que facilitan la conexión mediante equipos electrónicos o de radiofrecuencia (v.gr., conexiones de wi-fi, antenas para captura de ondas de radio u otros).

Desde una perspectiva práctica, lo primero que podría cuestionarse en relación con el empleo de estas aeronaves no tripuladas, es cuál es (o puede ser) su fin; cuál es su pretendida funcionalidad en cada caso, y, a su vez, convendrá saber qué tipo de información obtiene, cuál es su destino, dónde se registra y por quién o quiénes tendrá acceso a la misma. Pues, solo de este modo cabe pensar podrá identificarse posibles riesgos, o sus efectos directos o indirectos. Y, de este modo, una vez se disponga de dicho conocimiento previo, cabe proceder a evaluar cualquier tipo de uso de estos dispositivos, esto es, en atención a ponderar si fuera (o no) oportuno o resultara justificado. Si bien, ante este fenómeno, -como ante otros análogos-, parece recomendable aplicar los principios de precaución y de prevención[12], sobre todo cuando se trata de cuestiones sin certeza sobre sus consecuencias.

En especial, desde un enfoque jurídico, es relevante observar lo relativo a la eventual captación y procesamiento de información, datos, sonidos o imágenes que procede mediante este tipo de aparatos, en tanto hay que tener en cuenta lo dictado por el Ordenamiento europeo y nacional vigente, que así dispone un marco regulatorio común y vinculante en materia de protección de datos. No obstante, restaría por adoptar compromisos o acuerdos internacionales con el fin de

---

palabra para referir a esta tecnología por la semejanza observada entre ambos cuando vuelan y generan un ruido o zumbido característico.

[11] Cfr., Artículo 5. *Definiciones.* Real Decreto 1036/2017, de 15 de diciembre, por el que se regula la utilización civil de las aeronaves pilotadas por control remoto, y se modifican el Real Decreto 552/2014, de 27 de junio, por el que se desarrolla el Reglamento del aire y disposiciones operativas comunes para los servicios y procedimientos de navegación aérea y el Real Decreto 57/2002, de 18 de enero, por el que se aprueba el Reglamento de Circulación Aérea. (BOE núm. 316, de 29 de diciembre de 2017).

[12] El *principio de precaución* se cita en el artículo 191 del Tratado de Funcionamiento de la Unión Europea, si bien, "El principio de precaución no está definido en el Tratado, que sólo lo menciona una vez, para la protección del medio ambiente, pero, *en la práctica,* su ámbito de aplicación es mucho más vasto, y especialmente cuando la evaluación científica preliminar objetiva indica que hay motivos razonables para temer que los efectos potencialmente peligrosos para *el medio ambiente y la salud humana, animal o vegetal* puedan ser incompatibles con el alto nivel de protección elegido para la Comunidad". Al respecto, vid., Comunicación [COM(2000) 1 final] sobre el recurso al principio de precaución , texto disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=legissum%3Al32042. También, en la era digital, el principio de precaución recobra mayor valor, pues, en esencia su funcionalidad opera antes de producir un daño o evento adverso, incluso, con carácter previo al posible conocimiento o existencia de certeza absoluta alguna sobre posibles impactos negativos. Asimismo conviene diferenciar este principio, en sentido estricto, de otro esencial, el *principio de prevención*; este último, sí supone la pre-existencia de cierto conocimiento previo, o alguna certeza sobre la concurrencia de riesgos o la probabilidad de producirse eventos perniciosos, por lo que convendrá adoptar las oportunas medidas para evitar dicho daño. En suma, se actuará conforme a un proceso de causalidad caso de disponer de información previa, o con base a previa experiencia o el conocimiento adquirido, y, en síntesis, se ha de actuar en aras de evitar o prevenir el daño.

reforzar dicha protección, ya que las implicaciones que conllevan las TIC, en general, son globales, y, por ende, pueden desconocer las fronteras físicas, o ir más allá del ámbito de competencia y soberanía de cada Estado.

2.3. El Real Decreto 1036/2017.

En la actualidad, en nuestro Ordenamiento, en relación al uso civil de drones, hay que tener en cuenta lo dictado por el *Real Decreto 1036/2017, de 15 de diciembre, por el que se regula la utilización civil de las aeronaves pilotadas por control remoto, y se modifican el Real Decreto 552/2014, de 27 de junio, por el que se desarrolla el Reglamento del aire y disposiciones operativas comunes para los servicios y procedimientos de navegación aérea y el Real Decreto 57/2002, de 18 de enero, por el que se aprueba el Reglamento de Circulación Aérea*. Esta normativa, de forma expresa, reconoce que "Los avances científicos y técnicos han contribuido, en los últimos años, al progreso de la aviación permitiendo la aparición de estos vehículos aéreos no tripulados como nuevos usuarios del espacio aéreo. Esta circunstancia unida a la progresiva reducción de su coste de adquisición, ha permitido la proliferación de su uso de manera casi indiscriminada, con los consiguientes riesgos para la seguridad aérea"[13]. Por tanto, se procede a la actualización necesaria del marco regulatorio aplicable, hasta el momento, en materia de drones[14], y, a su vez, se pretende configurar un marco uniforme y común que aporte un nivel alto de seguridad "para fomentar el desarrollo del mercado de los UAS y para contribuir a mejorar la privacidad y la protección de datos"[15].

En consecuencia, este RD fija, en la actualidad, el marco jurídico definitivo aplicable al uso civil de drones, aeronaves pilotadas por control remoto (RPA), no sujetas a la normativa de la Unión Europea[16]. Esto es, aquellas aeronaves cuyo pilotaje es por control remoto (RPA) con masa

[13] Al respecto, el precitado RD 1036/2017, permite actualizar nuestra normativa en este ámbito, "En la línea del resto de los países de nuestro entorno, la modificación del artículo 11 de la Ley 48/1960, de 21 de julio, sobre Navegación Aérea, introducida por la Ley 18/2014, de 15 de octubre, de aprobación de medidas urgentes para el crecimiento, la competitividad y la eficiencia, estableció que estos artefactos son efectivamente aeronaves y, como tales, su utilización civil está sujeta a la legislación aeronáutica civil". Y, con todo, este RD, concreta el ejercicio de la habilitación normativa prevista en dicha Ley 18/2014 (art.50), que había fijado, con carácter temporal, el régimen jurídico aplicable a este tipo de aeronaves y a las actividades relativas a su empleo, hasta dictar la disposición reglamentaria prevista en su disposición final segunda, apartado dos (cf., artículo 509). Por lo que, este RD se dicta en ejercicio de dicha habilitación normativa, y, de este modo, "*establece el marco jurídico definitivo aplicable a la utilización civil de las aeronaves pilotadas por control remoto (RPA)*". No obstante, conforme señala, con esta norma "Se regula el régimen general aplicable en materia de matriculación y aeronavegabilidad, exceptuando, como ya lo hacía la regulación temporal vigente hasta la fecha, del cumplimiento de estos requisitos a las aeronaves pilotadas por control remoto (RPA) de hasta 25 kg de masa máxima al despegue, que, no obstante, están sujetas a condiciones específicas para su pilotaje". Y, por tanto, su ámbito quedaría limitado a lo expresado (cfr., Artículo 2. *Ámbito objetivo y subjetivo*). Así pues, se precisa que "Este real decreto, en coherencia con la convención internacional en la materia y las normas de derecho comparado no regula el uso de aeronaves civiles no tripuladas que no permiten la intervención del piloto en la gestión del vuelo, las denominadas aeronaves autónomas, cuyo uso en el espacio aéreo español y en el que España es responsable de la prestación de servicios de tránsito aéreo no está permitido".

[14] Este RD tiene por objeto de actualizar dicha regulación en lo relativo al uso del espacio aéreo y la acción potencial de aeronaves pilotadas por control remoto o RAPs.

[15] Tal y como señala el profesor Fernando González Botija, al analizar la normativa aplicable en eta materia y, en concreto, haciendo referencia a la Propuesta del Reglamento hoy vigente. Reglamento (UE) nº 2018/1139. Vid., GONZÁLEZ BOTIJA, F., "Los drones y la Unión Europea", *Revista española de derecho europeo* (REDE), nº. 65, 2018, pp. 37-71. De igual modo, resulta de interés observar la incidencia o el impacto de que este tipo de dispositivos puede implicar en relación con el deber de garantizar el pleno respeto y tutela pública de los derechos fundamentales, al respecto, GONZÁLEZ PUENTE, C. y GONZÁLEZ BOTIJA, F., "Los drones y los derechos fundamentales en la UE", *Revista Universitaria Europea* (RUE) nº 29. julio-diciembre 2018, pp. 77-114.

[16] Se regula lo relativo al el régimen de matriculación y aeronavegabilidad, salvo, en lo referente a las aeronaves pilotadas por control remoto-RPA de hasta 25 kg de masa máxima al despegue, pero que sí han de cumplir con los requisitos exigidos para su posible navegación. También, se fijan los necesarios condicionantes para poder proceder a la

máxima al despegue inferior a los 150 kg , asimismo con masa máxima al despegue superior, a las que no resulta aplicable el Reglamento (CE) nº 216/2008 del Parlamento Europeo y del Consejo de 20 de febrero de 2008, que determina las normas comunes en el ámbito de la aviación civil, y que crea una Agencia Europea de Seguridad Aérea. También deroga la Directiva 91/670/CEE del Consejo, destinadas a operaciones de aduanas, policía, búsqueda y salvamento, lucha contra incendios, guardacostas o similares. Y, por otra parte, se aplicará un régimen especial a las actividades u operaciones propias de Las Fuerzas y Cuerpos de Seguridad del Estado, así como de otros organismos públicos que prestan servicios de prevención, vigilancia y seguridad.

No obstante, este RD, conforme al Derecho internacional, no es aplicable al empleo de "aeronaves autónomas", aquellas aeronaves civiles no tripuladas sin la intervención del profesional o piloto para gestionar la navegación, que están prohibidas en el espacio aéreo español. Tampoco, este RD hace expresa referencia a la posible habilitación o autorización de otras actividades u operaciones con drones (RPA), destinadas a facilitar el transporte, u otras análogas, todo ello con base a razones preventivas y de seguridad.

En suma, la regulación que dicta este RD atiende, en cierta medida, a la demanda general existente en torno al uso de drones, y ello, con el propósito de asegurar que las prácticas efectuadas mediante de RPAs cumplan con unos estándares de seguridad adecuados, para usuarios y para terceros; asimismo con el fin de velar por la seguridad de las operaciones que tienen lugar en el espacio aéreo, si bien, todo ello conforme al estado de la técnica y el conocimiento científico disponible en el momento actual. En particular, resulta de interés, examinar los límites y condicionantes que esta regulación establece, en orden a cuestiones de seguridad pública, como son la necesaria identificación de este tipo de vehículos aéreos, -al ser las RPAs aeronaves que operan por control remoto-, y en relación con el debido cumplimiento de los requerimientos exigidos para operar con dichas aeronaves. En este sentido, hay que tener en cuenta el deber exigido relativo a la previa comunicación al Ministerio del Interior de acciones en áreas urbanas, o en escenarios poblados o donde existiera concurrencia de personas. Asimismo, en desarrollo del artículo 42 bis de la Ley 21/2003, de Seguridad Aérea, se determinan los deberes que han de cumplir los sujetos que emplearan RAPs para usos deportivos o recreativos, o análogos, con el fin de que no exista riesgo. De igual modo, hay que observar lo establecido por el Reglamento de Ejecución (UE) n.º 923/2012 de la Comisión, de 26 de septiembre de 2012, que dicta lo relativo a operaciones comunes para servicios y procedimientos de navegación aérea, modificando la normativa precedente, Reglamento de Ejecución (UE) n.º 1035/2011, y los Reglamentos (CE) n.º 1265/2007, (CE) n.º 1794/2006, (CE) n.º 730/2006, (CE) n.º 1033/2006 y (UE) n.º 255/2010, relativo a las aeronaves de juguete (aeronaves no tripuladas destinadas a juegos de menores de 14 años, o para usos similares). Además, se advierte que en caso de uso de este tipo de naves como "juguetes" se han de cumplir otros requerimientos adicionales, conforme ordena el Real Decreto 1205/2011, de 26 de agosto, sobre la seguridad de los juguetes.

Por último, en el ámbito europeo, hay que hacer especial referencia, por su importancia, al REGLAMENTO (UE) Nº 2018/1139, del Parlamento europeo y del Consejo de 4 de julio de 2018, sobre normas comunes en el ámbito de la aviación civil y por el que se crea una Agencia de la Unión Europea para la Seguridad Aérea[17]. Este texto normativo, vinculante, establece

---

explotación de este tipo de vehículos aéreos. En síntesis, sigue la legislación que opera en otros países, y que rige la utilización de este tipo de naves RPA para actividades de investigación científica, o trabajos profesionales especializados (aquellos destinados a efectuar acciones u operaciones especializadas, tal y como dicta el Ordenamiento de la UE.

[17] REGLAMENTO (UE) Nº 2018/1139, del PARLAMENTO EUROPEO y del CONSEJO de 4 de julio de 2018, sobre normas comunes en el ámbito de la aviación civil y por el que se crea una Agencia de la Unión Europea para la Seguridad Aérea y por el que se modifican los Reglamentos (CE) nº. 2111/2005, (CE) nº. 1008/2008, (UE) n.o 996/2010, (CE) nº. 376/2014 y las Directivas 2014/30/UE y 2014/53/UE del Parlamento Europeo y del Consejo y se derogan los Reglamentos (CE) nº. 552/2004 y (CE) nº. 216/2008 del Parlamento Europeo y del Consejo y el Reglamento (CEE) nº. 3922/91 del Consejo (DOUE núm. L 212/1, de 22-8-2018).

(Considerando 6) una serie de nuevos instrumentos de apoyo para la eficaz aplicación de "normas sencillas y proporcionadas a la aviación deportiva y recreativa". Con ello, se trata de propiciar que las medidas adoptadas sean de conformidad con este Reglamento, con el fin de disponer un marco regulatorio uniforme en la Unión Europea, que resulte aplicable a "este segmento del sector de la aviación" en todos los Estados miembros, y asegurando medidas que resulten proporcionadas/equilibradas, flexibles y rentables, conforme a las mejores prácticas existentes. Dichas medidas, por tanto, han de introducirse oportunamente y precisan de la colaboración entre Estados, con el fin de evitar discrepancias y cargas administrativas o financieras que fueran innecesarias o excesivas para los fabricantes y los operadores[18]. Por ende, la UE adopta un enfoque conciliador en torno al uso de drones, y no se ignora el potencial que también a nivel comercial supone este segmento del sector aeronáutico.

3. LA POSIBLE VULNERACIÓN DE DERECHOS FUNDAMENTALES: PRIVACIDAD Y PROTECCIÓN DE DATOS.

Por lo general, como se sabe la legislación suele ir con lentitud respecto a la rápida evolución de la innovación tecnológica y sus aplicaciones prácticas. En especial, lo mencionado se pone de manifiesto cuando se observan actividades donde se emplean nuevos dispositivos o aparatos electrónicos, así como otros artefactos o elementos fruto del desarrollo de la inteligencia artificial. En este contexto digital, uno de los aspectos que pueden verse afectados, en mayor medida, por el uso de nuevas tecnologías, es el relativo a la esfera de la privacidad y la protección de datos, tal y como ya ha sido expresado (*supra*). La cuestión no es baladí, al tratarse de derechos fundamentales reconocidos de los ciudadanos, por lo que resulta preciso insistir en el deber de cumplimiento de la regulación vigente en materia de protección de datos.

En este sentido, y a efectos de significar la regulación vigente destinada a la tutela del derecho fundamental a la protección de datos, a continuación se procede a detallar las principales aportaciones de la vigente normativa europea, el *Reglamento europeo general de protección de datos* (RGPD)[19], y, a su vez, en España, la *Ley Orgánica 3/2018, de Protección de Datos y Garantía de los derechos digitales*, de 5 de diciembre (LOPDyGDD)[20].

4. NORMATIVA EUROPEA VINCULANTE: EL *REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS* (RGPD).

El RGPD ha sido clave para fijar una sólida disciplina común aplicable en materia de protección de datos, asimismo habilita a los Estados miembros para establecer medidas coordinadas para ordenar y supervisar las prácticas que operen en el ámbito de la Unión Europea. Si bien, hay que señalar que el actual reconocimiento del derecho a la protección de datos no ha sido casual, ya que ha sido fruto de una positiva evolución hasta lograr su consolidación como derecho fundamental. Así, el derecho a la protección de datos se consagra como derecho fundamental por el Derecho de la Unión Europea (UE), siendo de forma expresa declarado en la Carta de los Derechos Fundamentales de la Unión Europea (Artículo 8 CDFE), asimismo en el Artículo 16.1 del Tratado de Funcionamiento de la Unión Europea (TFUE). Y, con base a dicho reconocimiento, ha sido preciso establecer un régimen regulatorio común y de carácter vinculante, el vigente RGPD

[18] Al respecto, vid., el detallado estudio sobre esta materia y normativa específica elaborado por GONZÁLEZ BOTIJA, F., *Los drones y el derecho de la Unión Europea*. Atelier, Barcelona, 2018.

[19] Reglamento (UE) 2016/679, del Parlamento europeo y de Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). DOUE L 119/1, de 4.5.2016.

[20] BOE núm. 294, de 6 de diciembre de 2018.

(precitado), que supera a la precedente Directiva 95/46/CE, con el propósito de reforzar la protección ofrecida; asegurando, con ello, un marco jurídico básico y uniforme, que a su vez pueda ser completado por cada Estado miembro. Lo cual, responde a la pretensión principal de protección, fijando para ello un cuadro de medidas de obligatorio cumplimiento, y, a su vez, evitando la diversidad normativa preexistente en esta materia.

De este modo, en materia de protección de datos, el Derecho de la Unión Europea ha consolidado un único régimen aplicable, de forma común, en virtud del vigente *Reglamento General de Protección de Datos* (RGPD, 2016), ya que resultó insuficiente a dicho fin la precedente Directiva comunitaria 1995/46 sobre Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y la Libre Circulación de estos datos.

4.1. Aportaciones del RGPD.

El actual RGPD incorpora destacadas novedades con el propiciar una adecuada tutela pública en materia de protección de datos. Este RGPD (2016) en vigor, -con plenos efectos desde el pasado mayo de 2018-, establece una serie de principios rectores aplicables al tratamiento de datos, que son de obligado cumplimiento. Asimismo, en España, completando a dicha normativa europea, ha sido promulgada la nueva *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales* (en vigor desde el 7 de diciembre de 2018). Esta Ley incorpora a su vez un innovador catálogo de derechos digitales, cuyo reconocimiento supone un hito jurídico, al sentar una base legal relativa a esta tipología específica de derechos, que requieren disponer de protección y garantías específicas.

4.2. El impacto de los drones y sus riesgos (acceso a información y datos personales sin autorización).

Conforme señala la normativa precitada, los *«datos personales»* comprenden todo tipo de *"información sobre una persona física identificada o identificable («el interesado»); se considerará 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*; (…)". Por ende, cualquier instrumento o procedimiento que posibilitara obtener y registrar información, imágenes, sonidos, datos de geolocalización, o cualquier otra fuente o tipología de señales electromagnéticas o análogas, que permitiera identificar o pudiera estar en relación con una persona, implica o conlleva el necesario tratamiento de datos. En consecuencia, al uso de drones le es aplicable la precitada normativa, vigente en materia de protección de datos (vid., *supra*).

De igual modo, cabe agregar otro elemento a tener en cuenta, los drones pueden obtener y ser herramientas que facilitarían el registro de información o datos, sin que previamente concurra el conocimiento del sujeto o ciudadano, y, por tanto, sin posibilidad de disponer de la autorización expresa (otorgada por el titular de los datos) que es exigida al respecto, tal y como ordena el actual RGPD (sobre esta cuestión, en ulterior epígrafe se detallan los deberes del operador).

Al respecto, ya alertaron las Autoridades europeas de protección de datos (Grupo de Trabajo del Artículo 29, del que forma parte la AEPD), en particular, sobre los riesgos que plantea el uso de drones[21] y como pueden afectar a la privacidad y protección de datos; haciendo hincapié

[21] El Grupo de Trabajo del Artículo 29, órgano consultivo independiente integrado por las autoridades europeas de protección de datos de todos los Estados Miembros (entre las que se encuentra la Agencia Española de Protección de Datos), el Supervisor Europeo de Protección de Datos y la Comisión Europea, emitió el 16 de junio de 2015, su primer *Dictamen sobre privacidad y cuestiones de protección de datos relativas a la utilización de drones* (vid., https://ec.europa.eu/newsroom/article29/news-overview.cfm). Cfr., "El Grupo de Trabajo del Artículo 29 se

en que estas aeronaves, equipadas con equipos receptores de imágenes y otros sensores, pueden "captar y procesar datos personales" (cf., primer Dictamen conjunto emitido, en el que se exponen riesgos relativos al uso de drones y asimismo se insiste en las obligaciones que deberían cumplirse por los operadores responsables)[22].

4.3. Tratamiento de datos: Principios rectores y aplicación del RGPD al uso de drones.

Tal y como ha sido observado, el empleo de drones, al implicar un posible tratamiento de datos, queda sujeto a la legislación de protección de datos precitada (RGPD y LOPDyGDD). A su vez, hay que atender a las propiedades de cada modalidad de dispositivo o artefacto empleado, en concreto, pues hoy existen distintas tipologías de drones y sus usos son diversos. Al ser vehículos aéreos puede ofrecer varias posibilidades a la hora de captar imágenes, u otros datos o información relativa a personas: vía vuelos en áreas urbanas, navegación nocturna, navegar en cierta áreas o espacios aéreos controlados, incluso, pudiera tratarse de vuelos fuera del alcance visual, etc.. Lo mencionado, además, podrá acontecer sin que pudiera ser advertido por los ciudadanos. En este sentido, hay que tener en cuenta lo dictado por el *Real Decreto 1036/2017, de 15 de diciembre,* (referenciado en el epígrafe precedente), que fija el nuevo marco normativo que regula el uso civil de este tipo de aeronaves pilotadas por control remoto, pero además hay que tener presente que también resulta aplicable directamente el RGPD.

En cualquier caso, queda claro cuál es la funcionalidad que puede identificar a este tipo de dispositivos, el obtener información, datos o imágenes, para posibilitar su posible registro y posterior tratamiento. En este sentido, ya advierte la Agencia Española de Protección de Datos (AEPD)[23], precisando que el uso de drones queda sujeto al cumplimiento de la legislación relativa al uso de cámaras de videovigilancia, cuando opere como dichas cámaras. Si bien, esta es solo una de las múltiples posibilidades que un dron puede ofrecer, ya que además el dron permite –como se sabe– más aplicaciones, usos o finalidades. Asimismo, también hay que considerar si la videovigilancia es realizada en lugares públicos o privados, pues ello es fundamental para observar cada supuesto, esto es, si la práctica o uso implicaría un posible tratamiento de datos de carácter personal. Por ende, además de la normativa en materia de videovigilancia resultará aplicable la específica, reguladora del empleo de drones.

Agregado a lo anterior, es necesario tener en cuenta la aplicación del precitado régimen jurídico (general) dictado en materia de protección de datos, que establece los presupuestos esenciales para el tratamiento de datos en la Unión Europea. De este modo, rige un cuadro preceptivo de "*Principios de la protección de datos*"[24], y se detallan derechos y deberes. En especial, hay

---

pronuncia sobre el uso de drones", en: https://blog.cuatrecasas.com/propiedad-intelectual/el-grupo-de-trabajo-del-articulo-29-se-pronuncia-sobre-el-uso-de-drones/

[22] Cfr., Vid., AEPD, "Las Autoridades europeas de protección de datos aprueban el primer Dictamen conjunto sobre drones", en: http://www.lopdat.es/noticias/las-autoridades-europeas-de-proteccion-de-datos-aprueban-el-primer-dictamen-conjunto-sobre (Fecha última consulta: 09/03/2019).

[23] AEPD, Gabinete jurídico, informe emitido con motivo de "La consulta ha sido planteada por una empresa que se define a sí misma en su consulta como "operador de drones". Dicha consulta solicita precisar lo relativo al contenido del *"dictamen sobre uso de drones realizado por la comunidad europea",* y, en particular, acerca de "*si es necesario gestionar el dron como una cámara de videovigilancia y por lo tanto dar de alta a éste con su archivo correspondiente o solamente es necesario realizar un estudio de impacto en la protección de datos*". Este informe es de interés, por cuanto examina la normativa aplicable a los drones, con base a sus propiedades y posibles funcionalidades. Texto del Informe disponible en: https://www.aepd.es/media/informes/informe-juridico-rgpd-drones.pdf; Asimismo, vid., https://www.aepd.es/media/informes/informe-juridico-rgpd-camaras-on-board.pdf

[24] Cf., Artículo 4 LOPD Calidad de los datos; y, en la actualidad, son enunciados los "principios relativos al tratamiento" en el Artículo 5 del nuevo Reglamento General de Protección de Datos (RGPD).

que destacar las obligaciones que deben ser observadas por los operadores en lo relativo al tratamiento de datos (Responsable y Encargado del tratamiento). Algunos de estos principios ya fueron previstos por la precedente Directiva 95/46/CE[25], y otros han sido incorporados por el nuevo Reglamento, completando así el Sistema regulatorio vigente.

En concreto, el vigente texto del RGPD dicta seis principios rectores, que en esta materia han de servir para disciplinar toda acción y proceso de gestión de la información y comunicación sobre datos personales; por ello, son de necesaria observancia dichos presupuestos en toda acción o proceso que suponga el tratamiento de datos personales. De este modo, el artículo 5 del RGPD enuncia dichos principios, desarrollados con precisión en los artículos 6 a 11. En síntesis, estos seis principios determinan lo siguiente,

- Los datos personales han de ser tratados de forma lícita, leal y transparente.
- Los datos personales deben ser recogidos con fines concretos, explícitos y legítimos.
- Los datos personales deben ser adecuados, pertinentes y limitados a la finalidad que motiva su tratamiento.
- Los datos personales deben ser veraces, exactos y actualizados.
- Los datos personales han de mantenerse de forma adecuada (custodia) y de forma que se pueda permitir su identificación y conocimiento por los interesados; además, dicho empleo, depósito o registro únicamente lo será por el tiempo máximo que fuera necesario para los fines del tratamiento.
- Los datos personales han de ser tratados de forma que se garantice su seguridad (gestión y prevención de riesgos).

Entre estos principios, hay que destacar el contenido del "principio de finalidad"[26], según del cual los datos han de ser recogidos para fines determinados (Art.5.1.b. RGPD), y, en consecuencia, únicamente se podrá recabar aquellos datos que fueran precisos para cumplir aquella finalidad que fuera anunciada (sobre lo que previamente se ha de informar a su titular, *cedente*). Por tanto, se ha de facilitar el ejercicio del derecho a la información que fuera necesaria o cuando lo solicitara persona legitimada para ello[27]. A su vez, se establece que para disponer de datos personales es preciso contar con el consentimiento de su titular; esto es, la autorización expresa (previa) para tratar (y/o ceder) datos es un requisito obligado. Debiendo hacer constar todo ello –por el operador– al que hubieran sido cedidos dichos datos, y a los efectos informados. Este principio, por ende, supone un presupuesto preliminar que resultará idóneo para evaluar la adecuación (o no) de cada práctica; y, en particular, en orden a poder valorar/acreditar el grado de cumplimiento exigido a cada operador u operadores obligados (entidad, empresa o profesional) conforme dicta el vigente RGPD[28] (y, en el mismo sentido, dicta la actual Ley española 2018, LOPDyGDD, vid., Título II. *Principios de protección de datos*, arts. 4 a 10, y art. 11 dentro del Título III. *Derechos de las personas*).

Por tanto, el empleo de drones implica gestionar la información que a través de estos aparatos o sus equipos vinculados se facilitara conforme a lo dictado por la citada normativa. Así, la

[25] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DOCE n" L 281 /31, de 23-11-95).

[26] Sentencia del Tribunal de Justicia (Gran Sala) de 13 de mayo de 2014. Procedimiento/Asunto - C-131/12 - EU:C:2014:317, Google Spain y Google. Disponible en: http://curia.europa.eu/juris/liste.jsf?num=C-131/12

[27] En lo relativo al deber de información al interesado, cfr., artículo 13 RGPD, "*Información que deberá facilitarse cuando los datos personales se obtengan del interesado*", diferenciando cuando se tratara de aquella otra *información que no se hubiera obtenido del interesado* (art. 14) . Asimismo, se reconoce el *derecho de acceso del interesado* (Art. 15).

[28] A efectos prácticos, resulta ilustrativo consultar, AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD), "Guía del Reglamento General de Protección de Datos para responsables de tratamiento". Madrid 2018. Disponible en: https://www.aepd.es/media/guias/guia-rgpd-para-responsables-de-tratamiento.pdf

AEPD hace hincapié en observar con qué finalidad es empleado el dron, por lo que es de interés determinar la "legitimación limitada", en cada caso, conforme al deber de cumplir con los expresados *Principios relativos al tratamiento de datos,* Artículo 5 del RGPD. Siendo en todo caso, el operador responsable del tratamiento, el que deberá acreditar dicho cumplimiento («responsabilidad proactiva»). Y, de este modo, cabe interpretar que cuando con el uso del dron se registren imágenes, con fin de videovigilancia, y afectara a espacios privados, le será de aplicación el RGPD; siendo así aplicable lo relativo al deber/derecho de información (artículo 13), y, a su vez, el deber de registro de actividades de tratamiento (artículo 30), el deber de implementar sistemas adecuados de análisis y prevención de riesgos, junto con los protocolos de de seguridad necesarios (artículo 32), que corresponderá observar al operador/es responsable (correspondiendo a ellos acreditar dicho cumplimiento).

No obstante, cabe advertir sobre la problemática que, en la práctica real, pudiera surgir en lo relativo al ejercicio del *derecho de acceso a la información* (art.15 RGPD)*,* por parte del interesado, ya que pudiera obstaculizarse por el operador/es. En este sentido, el cumplimento del *deber de informar* pudiera ser difícil de exigir o reclamar por el interesado; en esta cuestión hay que tener en cuenta lo previsto en el artículo 14.5 RGPD, ya que, en efecto, plantearía dificultades en ciertos supuestos, caso de alegarse la imposibilidad técnica o por falta de viabilidad de facilitar información, por suponer un alto coste para el operador, por ejemplo. Si bien, corresponderá al operador justificar dichas eventualidades, por ser clara dicha normativa, al establecer el deber de informar al interesado a cargo del responsable del tratamiento, o, en su defecto, se deberá facilitar otras posibles vía de conocimiento o acceso a información (vía posibles medios de constancia o publicación). También hay que tener en cuenta que caso de incumplimiento, resultaría de aplicación el régimen de infracciones y sanciones previsto en el RGPD.

4.4. Deberes de los operadores.

Entre las obligaciones que afectan a los sujetos u operadores responsables del tratamiento de datos (v.gr., entidades, empresas y profesionales), cabe destacar:

- La designación necesaria del sujeto que actuara como *Delegado de Protección de Datos* (DPD). El RGPD obliga a quien gestione o realizara tratamiento de datos, a designar a esta figura, que ha de ser un profesional experto, con una formación específica y acreditada, tanto en protección de datos personales como en análisis de riesgos y medidas de seguridad de la información, y que podrá ser personal interno o externo a la entidad[29].
- La *obligación de registrar documentalmente las acciones y procesos de tratamiento.* Dicho deber, corresponde tanto a los Responsables de ficheros como a los Encargados del tratamiento de datos (figuras definidas en el Artículo 4, apartados 7 y 8).
- El tratamiento de datos personales *exige disponer del previo consentimiento expreso por parte del titular de los datos***.** En consecuencia, ya no es suficiente con un consentimiento tácito, por lo que los operadores o empresas quedan obligadas a solicitar dicho consentimiento y asegurar su constancia, también respecto a los datos previos de que dispongan (antes de la entrada en vigor del RGPD).
- Es necesario implementar métodos de *evaluación de impacto y análisis de riesgos*, en relación con el tratamiento requerido y conforme a cada tipología de datos, así como disponer de las oportunas medidas preventivas y de seguridad.
- Se insiste en el cumplimiento de los deberes de *transparencia informativa.*
- Se establece la *obligación de notificar cualquier tipo de vulneración de los sistemas de seguridad* implementados relativos los datos personales. Así, en plazo máximo de 72 horas, se deberá comunicar cualquier eventualidad que sucediera a la Agencia Española de Protección de Datos

[29] Sobre la funcionalidad y el perfil de esta figura, vid., LOZANO, S. (AENOR), "El Delegado de Protección de Datos, el profesional más buscado", *Revista AENOR* nº 340, septiembre 2018, pp. 24-27.

(AEPD), y de igual modo, en casos graves será necesario notificarlo a los afectados o interesados, con el fin de evitar mayores daños o perjuicios.

- Revisión y/o re-configuración de los *modelos contractuales*. Conforme dicta el RGPD, será preciso revisar los instrumentos contractuales vigentes, así como diseñar nuevos modelos contractuales asegurando que cumplen con el RGPD. De igual modo, será necesario proceder a realizar nuevos contratos con los encargados de tratamiento, en cuyo clausulado se ha de prestar especial atención en lo relativo a las facultades de acceso a datos por terceros (respetando lo previsto como "contenido mínimo necesario").

Por otra parte, hay que señalar que el texto del RGPD, en principio, no diferencia entre datos personales y datos profesionales, por lo que cabe interpretar que las empresas han de adoptar las oportunas acciones en atención a cada perfil y categoría de datos, con el fin de asegurar el cumplimiento de los deberes exigidos.

4.5. Derechos de los ciudadanos.

A su vez, el RGPD amplía el conjunto de derechos que podrá ejercer el interesado, así junto a los ya reconocidos por la previa Directiva 95/46/CE se incorporan otros nuevos: *derecho de acceso, derecho a la portabilidad de datos, derecho de cancelación, derecho de rectificación, derecho de oposición*, y *el "derecho al olvido"*. En particular, con referencia al "derecho al olvido", hay que señalar que esta facultad, en la práctica, supone una manifestación de los *derechos de cancelación u oposición en el entorno digital u online.* No obstante, este derecho no es absoluto, ya que podrá atender a ciertas limitaciones, con base al ejercicio de otros derechos, como son: la libertad de expresión, el derecho a la información, el interés público en el ámbito de la salud, la investigación, y en caso de reclamaciones o recursos[30].

Asimismo, de forma específica, se reconoce el "*derecho a la limitación del tratamiento*", y el "*derecho a no ser objeto de decisiones individualizadas*", de forma que no se podrán adoptar decisiones que incluyan medidas no consentidas de forma expresa por el interesado, cuando estas evalúen o valoren aspectos personales, o con referencia a la persona, o en caso de medidas basadas en tratamiento automatizado y que pudieran generar perjuicios o efectos jurídicos perniciosos para el titular de los datos, o le afectaran de forma grave.

5. REFERENCIA A LA "CARTA DE DERECHOS DIGITALES" (Ley Orgánica 3/2018, de 5 de diciembre).

El texto del RGPD otorgaba el plazo de dos años para que los Estados miembros procedieran a la revisión y actualización de su respectiva legislación en materia de protección de datos, con el fin de adecuarla a este nuevo régimen jurídico europeo. Y, de este modo, en España, es promulgada la *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los derechos digitales* (LOPDyGDD)[31], en vigor desde el 7 de diciembre de 2018 (D.F.16ª).[32]

---

[30] Al respecto, vid., Considerando 4 RGPD, "(…) *El derecho a la protección de los datos personales no es un derecho absoluto sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad".*

[31] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE núm. 294, de 6 de diciembre de 2018). Este texto legal y normativa precedente en esta materia, puede ser consultada en: https://www.boe.es/legislacion/codigos/codigo.php?id=55&modo=1&nota=0 . Y, con carácter previo, se aprobó el Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos (BOE núm. 183, de 30/07/2018, vid., https://www.boe.es/buscar/act.php?id=BOE-A-2018-10751, disposición derogada con la aprobación de la vigente Ley, precitada.

Esta Ley demuestra ser conforme al RGPD, e innovadora, pues desarrolla y complementa a dicto Reglamento. Además, como novedad, incluye, -por vez primera en nuestro Ordenamiento-, la declaración de una serie de derechos digitales que incorpora en el Título X "Garantía de los derechos digitales". Dicha declaración opera a modo de catálogo legal o "Carta de derechos digitales", lo que supone un hito jurídico relevante en nuestro Sistema jurídico, que asimismo podrá servir de modelo para otros Ordenamientos. En este sentido, hay que significar que esta "*Carta de derechos digitales*" pretende promover que asimismo se puedan implementar los oportunos desarrollos y acciones para dar efectividad a este tipo de derechos de la ciudadanía. Lo que parece oportuno en la era digital y, sobre todo, ante el mayoritario empleo de Internet, y el incremento de prácticas en los actuales (o futuros) entornos tecnológicos. Por ende, la transformación digital conlleva el reconocimiento de determinados derechos, aportar mayor seguridad jurídica ante la diversidad de herramientas tecnológicas o digitales empleadas en comunicación y prestación de servicios.

En consecuencia, el contenido del Título X (artículos 79 a 97) contiene la declaración de los siguientes derechos digitales: Artículo 80. *Derecho a la neutralidad de Internet.* - Artículo 81. *Derecho de acceso universal a Internet.* - Artículo 82. *Derecho a la seguridad digital.* - Artículo 83. *Derecho a la educación digital.* - Artículo 84. *Protección de los menores en Internet.* - Artículo 85. *Derecho de rectificación en Internet.* - Artículo 86. *Derecho a la actualización de informaciones en medios de comunicación digitales.* - Artículo 87. *Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral.* - Artículo 88. *Derecho a la desconexión digital en el ámbito laboral.* Artículo 89. *Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo.* - Artículo 90. *Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral.* - Artículo 91. *Derechos digitales en la negociación colectiva.* - Artículo 92. *Protección de datos de los menores en Internet.* - Artículo 93. *Derecho al olvido en búsquedas de Internet.* Artículo 94. *Derecho al olvido en servicios de redes sociales y servicios equivalentes.* - Artículo 95. *Derecho de portabilidad en servicios de redes sociales y servicios equivalentes.* Artículo 96. *Derecho al testamento digital.* - Artículo 97. *Políticas de impulso de los derechos digitales.*

Con la incorporación de este título específico, la actual Ley española de protección de datos es pionera en el reconocimiento de esta nueva generación de derechos relativos al entorno virtual. No obstante, debe observarse que algunos de estos derechos ya constan en otras disposiciones normativas, o bien, suponen adaptaciones o reformulaciones al presente entorno digital de derechos fundamentales consagrados por nuestro Ordenamiento. Por último, la Ley dicta que el Gobierno, en colaboración con las Comunidades Autónomas, deberá elaborar un Plan de medidas de actuación relativo al "Acceso a internet", conforme a los objetivos que esta Ley detalla, y con la finalidad de promover próximas "Políticas de impulso de los derechos digitales" (art. 97). Asimismo le encomienda la aprobación de un Plan de Actuación destinado a fomentar acciones formativas/educativas y de sensibilización[33].

---

[32] Este texto legal ha sido aprobado por nuestras Cortes Generales por unanimidad. Si bien, cierto es que este texto legal ha sido dictado con posterioridad al plazo de dos años previsto por el Reglamento europeo (Art. 99 RGPD) para adaptar las legislaciones nacionales al RGPD. Cfr., 121/000013 Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal. BO. Cortes Generales - Congreso de los Diputados, núm. 13-3, 9 de octubre de 2018, pág.1. http://www.congreso.es/public_oficiales/L12/CONG/BOCG/A/BOCG-12-A-13-3.PDF. Al respecto, vid., noticia publicada con fecha 21.11.2018 http://www.rtve.es/noticias/20181121/senado-aprueba-nueva-ley-proteccion-datos-derechos-digitales/1841709.shtml).

33 Con el propósito de que "*los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales y de las redes sociales y de los servicios de la sociedad de la información equivalentes de Internet con la finalidad de garantizar su adecuado desarrollo de la personalidad y de preservar su dignidad y derechos fundamentales*". Y, por otra parte, el apartado 3 de este artículo, señala que el Gobierno ha de elaborar el correspondiente informe anual acerca de la aplicación de esta Ley, que remitirá a la comisión parlamentaria correspondiente del Congreso de los Diputados, con el fin de poder valorar la evolución de la misma y sobre su impacto o efectos, así como observar medidas o propuestas en materia de derechos digitales.

6. MARCO DE RESPONSABILIDAD DE LOS OPERADORES.

Con referencia al marco de responsabilidad del operador u operadores, en lo relativo al empleo de drones, y conforme a la aplicación del la normativa vigente en materia de protección de datos (precitada), cabe señalar que la cuestión puede ser compleja en la práctica. Por cuanto, es posible supuestos en que existiera la participación de varios sujetos operadores/responables, y con ello ,la concurrencia de responsabilidades. Por ende, en atención a cada caso, conviene precisar la diferencia entre las competencias que corresponden, en principio, a dos posibles figuras o profesionales, en materia de tratamiento de datos, estos son: el operador "Responsable del tratamiento" de datos, y el "Encargado", al que se le encomienda la práctica de dicho tratamiento, y con motivo de la ejecución de una actividad o servicio contratado (por ejemplo, el empleo de drones para prestar un servicio destinado a cumplir una finalidad determinada).

6.1. El *Responsable* y el *Encargado* del tratamiento de datos.

El artículo 4, del RGPD, apartados 7 y 8, aporta la noción correspondiente a dichos sujetos: el "Responsable del tratamiento", es la persona física o jurídica, entidad o autoridad pública, que ordena el empleo del dron, y, al efecto, organiza la infraestructura necesaria y establece el modo, la finalidad y medidas empleadas para el tratamiento de datos; y, por otra parte, el "Encargado", es la persona física o jurídica, entidad, autoridad pública, servicio u otro organismo que implementa lo encomendado por el Responsable, y, procede a la práctica de dicho tratamiento de la información obtenida (o datos personales), conforme a cumplir con las instrucciones que le facilitara dicho Responsable. Esto es, el operador responsable es el director y organizado del proceso y actuaciones, actuando bajo dicha encomienda del operador encargado.

Si bien, el RGPD (artículo 32) establece, de forma expresa, que, ambos sujetos quedan obligados a cumplir esta normativa, y, por tanto, son responsables en lo relativo al tratamiento de datos. Por lo cual, deberán adoptar todas las medidas oportunas (detalladas *infra*), de igual modo, procederá respecto a los empleados, agentes o profesionales que actuarán bajo la dirección de dichos sujetos.

En consecuencia, el responsable y el encargado del tratamiento deben adoptar todas las medidas necesaria para asegurar que aquellos empleados, profesionales o colaboradores (por ej., también en caso de subcontratación de servicios) que actuaran bajo su dirección o encomienda, y que, por ello, pudieran tener conocimiento o acceso a datos personales, cumplan con la normativa y adopten todas las medidas necesarias para la protección de los datos tratados. En suma, todos estos posibles sujetos han de proceder con diligencia y seguir las orientaciones dictadas por el operador *responsable*. Esto es, el respeto a la legislación vigente obligaría a todos los agentes, por lo que será importante prestar atención a lo estipulado en cada contrato o instrumento jurídico que vinculara a las partes o sujetos que intervienen en aquellas actividades o prestación de servicios que incluyan, de forma directa o indirecta, el tratamiento de datos.

6.2. Requerimientos específicos en materia de gestión, análisis de riesgos y seguridad en el tratamiento de datos.

Las Autoridades europeas de protección de datos (Grupo de Trabajo del Artículo 29, del que forma parte la AEPD), pusieron de manifiesto sobre los riesgos existentes con motivo del uso de drones[34],

[34] El Grupo de Trabajo del Artículo 29, órgano consultivo independiente integrado por las autoridades europeas de protección de datos de todos los Estados Miembros (entre las que se encuentra la Agencia Española de Protección de Datos), el Supervisor Europeo de Protección de Datos y la Comisión Europea, emitió el 16 de junio de 2015, su primer *Dictamen sobre privacidad y cuestiones de protección de datos relativas a la utilización de drones* (vid., https://ec.europa.eu/newsroom/article29/news-overview.cfm). Cfr., "El Grupo de Trabajo del Artículo 29 se pronuncia sobre el uso de drones", en: https://blog.cuatrecasas.com/propiedad-intelectual/el-grupo-de-trabajo-del-articulo-29-se-pronuncia-sobre-el-uso-de-drones/

-tal y como ha sido avanzado-, y, en concreto, en lo relativo a la privacidad y la protección de datos. Haciendo hincapié en que estas aeronaves pueden incorporar equipos receptores de imágenes y otros sensores, por lo que pueden "captar y procesar datos personales". Al respecto se elaboró un primer informe jurídico, Dictamen conjunto sobre drones, precisando las consideraciones oportunas, así como aquellas obligaciones que deberían cumplirse[35]. En dicho documento se examina el impacto que genera este tipo de aparatos en relación con la privacidad, y también aporta un conjunto de recomendaciones al respecto (destinadas a reguladores, fabricantes y operadores, incluso para las entidades o autoridades de vigilancia y control, v.gr., aduaneras, salvamento marítimo, otras). Pues, los drones hoy son empleados para distintos fines de vigilancia, supervisión costera, control del estado de infraestructuras, eventos, etc.

Con todo, dicho informe tenía como propósito promover un marco regulatorio común satisfactorio que regulara el empleo de drones, por cuanto era necesario adoptar un régimen uniforme y eficaz (al resultar insuficiente y dispersa la normativa existente hasta aquel momento, en los Estados miembros de la UE). Con ello, si bien se ponen en valor las ventajas que puede aportar el empleo civil de estos aparatos, de carácter social y económico, también se alerta sobre sus riesgos. De forma específica, entre ellos, se señala las posibles deficiencias en materia de transparencia informativa[36]. A ello, cabe sumar, los riesgos relativos a la posible vulneración de libertades y derechos, inclusive, cuando el empleo de drones fuera para fines lícitos, v.gr., seguridad y vigilancia de espacios públicos. De este modo, en especial, se subraya como relevante el asegurar la transparencia y el derecho a la información, así como, el deber de observar los principios de proporcionalidad, calidad y minimización de datos; y, con todo, se insiste en la necesidad de observar buenas prácticas en materia de tratamiento de datos.

Este Grupo de trabajo aportó una guía facilitadora que aproxima la interpretación adecuada de la normativa sobre protección de datos[37] en relación al empleo de drones. Entre otras recomendaciones, algunas de ellas tienen como destinatarios específicos a los principales grupos de interés, incluso a los fabricantes y/o distribuidores de estos aparatos, en tanto deberían diseñar modelos con menor riesgo, a fin de minimizar eventuales impactos y asegurando no afectar a la privacidad, y de igual modo, se señala la oportunidad de incluir guías de uso para usuarios, entre otras advertencias que fueran necesarias para el buen uso de estas aeronaves.

En particular, ya en este Dictamen se hace hincapié en el cumplimiento de la normativa en materia de protección de datos, que deberá ser considerada por las legislaciones nacionales dictadas para regular el uso comercial de drones. Asimismo, es necesario, en este ámbito, la cooperación entre autoridades competentes, nacionales y europeas, tanto en el ámbito de protección de datos como en aviación civil.

En la actualidad, conforme al RGPD, el empleo de drones precisa observar el cumplimiento de los principios del Art.5.1. RGPD; así pues, los datos han de ser: (a) tratados de forma lícita, leal y transparente; (b) obtenidos de forma legítima, destinados a fines concretos, y comunicado a los titulares/interesados; y, (c) el tratamiento de los datos ha de ser coherente con las finalidades previstas y anunciadas. Al respecto, rige el principio de "limitación de finalidad", y asimismo, hay que considerar determinadas "*Garantías y excepciones aplicables al tratamiento con fines de*

---

[35] Cfr., Vid., AEPD, "Las Autoridades europeas de protección de datos aprueban el primer Dictamen conjunto sobre drones", en: http://www.lopdat.es/noticias/las-autoridades-europeas-de-proteccion-de-datos-aprueban-el-primer-dictamen-conjunto-sobre (Fecha última consulta: 09/03/2019).

[36] Ya que este tipo de aeronaves no tripuladas pueden operar en distintos lugares o zonas, incluso con nocturnidad, sin que ello pueda ser advertido; de igual modo, advierte sobre la complejidad de su identificación de los operadores, equipos técnicos que fueran empleados para el tratamiento de datos, ni sobre el destino de la información o datos recabados con motivo de la navegación del dron, entre otros aspectos que son relevantes

[37] AEPD, "Guía del Reglamento General de Protección de Datos para responsables de tratamiento". Disponible en: https://www.aepd.es/media/guias/guia-rgpd-para-responsables-de-tratamiento.pdf

archivo en interés público, fines de investigación científica o histórica o fines estadísticos" (art. 89)[38]. Además, se insite en que solo se podrá recabar aquellos datos que fueran necesarios, esto es, adecuados, pertinentes y limitados en virtud de los fines predispuestos. Asegurando que el tratamiento de datos procede conforme con seguridad y en atención al principio de "minimización de datos".

Observando todo lo expresado, se infiere que la licitud del tratamiento de los datos ha de ser ponderada en cada caso, y dependerá del grado de cumplimiento observado con respecto a los mencionados principios; al ser estos presupuestos ordenados por el RGPD. En su defecto, podrán ser sujetos responsables, tanto el propio Responsable como el Encargado del tratamiento (art. 28 RGPD). Y, en cualquier caso, a ellos corresponderá acreditar la satisfactoria implementación de los oportunos sistemas de gestión, medidas, acciones y procesos de tratamiento de datos. Lo cual, adquiere especial relevancia, al operar mediante drones, lo relativo a equipos técnicos y medidas de prevención de riesgos y de seguridad. Lo que incluye la ciberseguridad (evitando posibles ataques que trataran de obtener el dominio del aparato o sus equipos remotos, o fuentes de registro de la información, etc).

Con todo, se señala en el propio texto del RGPD que "*Las personas físicas deben tener el control de sus propios datos personales"*, y, por tanto, *"Hay que reforzar la seguridad jurídica y práctica para las personas físicas, los operadores económicos y las autoridades públicas*" (Considerando 7). Con base a esta consideración, el legislador europeo ha reforzado las medidas exigidas y los deberes que han de cumplir los operadores (Responsables y Encargados) en lo relativo al tratamiento de datos. Esta cuestión ha sido principal para la Unión Europea, por su interés jurídico, y también por la incidencia que mantiene en relación con el esperado buen desarrollo del mercado. De forma expresa el vigente RGPD, en su artículo 1.3., dice, "*La libre circulación de los datos personales en la Unión no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales*"[39]**.** Sin duda, era preciso diseñar una normativa que permitiera conciliar la protección de datos y, por otra parte, el ejercicio del derecho a la libertad de información (veraz)[40].

El RGPD subraya, "*en particular el respeto de la vida privada y familiar, del domicilio y de las comunicaciones, la protección de los datos de carácter personal, la libertad de pensamiento, de conciencia y de religión, la libertad de expresión y de información (…)*". Y, a su vez, se señala que cabe la posible delimitación del derecho a la protección de datos, por cuanto este derecho no es un derecho absoluto; ergo, en su consideración y aplicación procede encontrar el equilibrio con otros derechos fundamentales, en atención al *principio de proporcionalidad* (Considerando 4). No obstante, el RGPD precisa que las posibles limitaciones a su ejercicio han de estar previstas legalmente, observando los criterios comunes fijados por esta normativa, y además, han de ser implementadas con base a instrumentos y medidas que se dictaran por cada Estado, respetando unos criterios uniformes, y en todo caso, garantizando el principio de legalidad y seguridad jurídica, así como el principio de transparencia

---

[38] Cfr., Art. 89.1. RGPD, "1. *El tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos estará sujeto a las garantías adecuadas, con arreglo al presente Reglamento, para los derechos y las libertades de los interesados. Dichas garantías harán que se disponga de medidas técnicas y organizativas, en particular para 4.5.2016 L 119/84 Diario Oficial de la Unión Europea ES garantizar el respeto del principio de minimización de los datos personales. Tales medidas podrán incluir la seudonimización, siempre que de esa forma puedan alcanzarse dichos fines. Siempre que esos fines pueden alcanzarse mediante un tratamiento ulterior que no permita o ya no permita la identificación de los interesados, esos fines se alcanzarán de ese modo*". (Nota: lo subrayado corresponde al autor).

[39] Lo dictado en este sentido por el RGPD, cuenta con precedentes en el Derecho comunitario europeo, ya que el tratamiento y circulación de información relativa a datos personales fue objeto de la Directiva 95/46/CE (cf., artículo 1.2.), señalando que la libre circulación de datos entre los Estados no debía ser prohibida o afectada por restricciones –en principio–, por lo que ha de resultar compatible con la pretendida protección de datos. Vid., referencia expresa realizada por HERRRÁN ORTIZ, A.I., "El derecho a la protección de datos en la sociedad de la información", *Cuadernos Deusto de Derechos Humanos*, op. cit., págs. 22-51 (en concreto, p. 22).

[40] Con respecto al requisito exigido de la veracidad, es contundente nuestro Ordenamiento español al consagrar en la Constitución española el derecho fundamental a la información, cf., Artículo. 20.1.d.) del Texto Constitucional, 1978.

informativa. En este aspecto insiste el RGPD, y también en relación con el régimen de control y supervisión que opere en cada Estado, así como en lo relativo a establecer vías para posibles reclamaciones y recursos, asimismo acerca de la articulación de un régimen sancionador específico, entre otras posibles herramientas que habilitara cada Estado para la tutela del DPD[41]. Por lo que respecta a posibles restricciones, determina que han de ser motivadas, ponderando su aplicación en cada caso y debida justificación; ya que en una sociedad democrática se ha de asegurar que cualquier eventual limitación relativa a derechos/libertades fundamentales ha de ser razonada, congruente e indispensable, cumpliendo con el principio de proporcionalidad[42].

En todo caso, el tratamiento de datos de carácter personal ha de respetar las libertades y derechos fundamentales. El RGPD, con todo, "*pretende contribuir a la plena realización de un espacio de libertad, seguridad y justicia y de una unión económica, al progreso económico y social, al refuerzo y la convergencia de las economías dentro del mercado interior, así como al bienestar de las personas físicas*" (Considerando 2 RGPD).

Por otra parte, también el propio RGPD advierte sobre la necesidad de observar en determinados casos la concurrencia de razones de interés público, que como tales han de primar (por lo que sí cabe aplicar posibles excepciones al régimen general previsto por el vigente RGPD). En este sentido, se señala que cuando exista un interés público "*deben*" autorizarse excepciones a la prohibición de tratamiento, relativo a ciertas categorías especiales de datos personales cuando así lo determinara el Derecho de la Unión o de los Estados miembros, "*siempre que se den las garantías apropiadas, a fin de proteger datos personales y otros derechos fundamentales*"[43].

Por último, es necesario señalar que el RGPD ha supuesto una revisión y actualización de otras normativas europeas dictadas que establecían directrices acerca del régimen aplicable al tratamiento de determinadas tipologías de datos, como la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas[44].

6.3. Medidas y sistemas de acreditación.

El Artículo 32 RGPD ("*Seguridad del tratamiento*"), señala que tanto el Responsable como el Encargado del tratamiento, deberán adoptar la medidas oportunas para asegurar las medidas de seguridad oportunas, "1.*Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos*

---

[41] Vid., Considerando 129, "(…) *Los Estados miembros pueden especificar otras funciones relacionadas con la protección de datos personales con arreglo al presente Reglamento. Los poderes de las autoridades de control deben ejercerse de conformidad con garantías procesales adecuadas establecidas en el Derecho de la Unión y los Estados miembros, de forma imparcial, equitativa y en un plazo razonable. En particular, toda medida debe ser adecuada, necesaria y proporcionada con vistas a garantizar el cumplimiento del presente Reglamento, teniendo en cuenta las circunstancias de cada caso concreto* (…/…)". (Nota: lo subrayado corresponde al autor).

[42] En este sentido, se ha pronunciado la jurisprudencia y de forma expresa el TEDH. Al respecto, vid., BARNÉS VÁZQUEZ, J., "El principio de proporcionalidad", *Cuadernos de Derecho Público*, 5, Instituto Nacional de Administración Pública, Madrid, 1998.

[43] Por ejemplo, caber interpretar así por razones de seguridad, supervisión, investigación de infracciones o delitos, salud pública, y también en el ámbito de la legislación laboral, protección social, pensiones, entre otros. (vid., Considerandos 52, 54, 55 y 56).

[44] Directiva sobre la privacidad y las comunicaciones electrónicas. (DO L 201 de 31.7.2002, p. 37). Al respecto, cfr., lo señalado por el Considerando 173 del RGPD, "*El presente Reglamento debe aplicarse a todas las cuestiones relativas a la protección de los derechos y las libertades fundamentales en relación con el tratamiento de datos personales que no están sujetas a obligaciones específicas con el mismo objetivo establecidas en la Directiva 2002/58/CE del Parlamento Europeo y del Consejo (2), incluidas las obligaciones del responsable del tratamiento y los derechos de las personas físicas. Para aclarar la relación entre el presente Reglamento y la Directiva 2002/58/CE, esta última debe ser modificada en consecuencia. Una vez que se adopte el presente Reglamento, debe revisarse la Directiva 2002/58/CE, en particular con objeto de garantizar la coherencia con el presente Reglamento".*

y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, (…)", que, entre otras, pueden ser,

a) *la seudonimización y el cifrado de datos personales;*

b) *la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento*;

c) *la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico*;

d) *un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento*.

Siendo para ello, además necesario proceder, con carácter previo, al análisis del riesgo, por parte de estos sujetos, operadores responsables, Art.32. 2., "*Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos*." Y, por otra parte, también se hace referencia a la necesidad de adoptar modelos de autorregulación, tal y como señala este artículo, en su apartado "3. La adhesión a un código de conducta" (cf., en relación con el Art. 40); seguir sistemas de auto-evaluación y certificación (artículo 42), como medios para poder acreditar el cumplimiento de los requisitos exigidos por este Art. 32.1. Y, agregado a lo anterior, el apartado 4 del art. 32, hace expresa referencia a la responsabilidad específica del operador: el *Responsable* del tratamiento de los datos, asimismo del *Encargado* de los mismos, con respecto a las personas que actuaran a su cargo, o subcontratadas, "4. *El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros*." (cfr., asimismo con lo previsto en el Art 29, "*Tratamiento bajo la autoridad del responsable o del encargado del tratamiento*").

En consecuencia, lo mencionado a su vez dependerá, como en otras innovaciones, del estado de la técnica en cada momento, de los costes de aplicación, así como de la naturaleza y el alcance con que opere, y del contexto y finalidad con que se proceda. Siendo la finalidad del tratamiento, una cuestión que debe quedar identificada (cf., art. 32.1. "*Seguridad del tratamiento*")[45]. En consecuencia, los operadores responsables quedan obligados a adoptar las medidas preventivas y de seguridad que fueran necesarias para evitar dichos daños[46]. Asimismo, cabe interpretar que dichos sujetos, en su caso, responderán ante posibles externalidades negativas que pudiera generar la actividad que desarrollan empleando drones, ya sea de forma directa o indirecta. Si bien, aquí puede plantearse alguna dificultad probatoria, cuando los daños fueran detectados a lo largo del tiempo, o cuando no existiera constancia sobre el registro o aplicación posterior de los datos obtenidos, y, en su caso, hubieran sido cedidos a terceros, sin consentimiento.

En cualquier caso, con respecto al deber de cumplir con las medidas y obligaciones mencionadas, el RGPD es contundente, al determinar que la responsabilidad corresponderá tanto del responsable como al encargado del tratamiento de datos; por lo que ambos sujetos han de actuar con suma diligencia, y aplicar aquellos sistemas de gestión e instrumentos técnicos que sean necesarios, con el fin de asegurar un nivel de seguridad adecuado (en coherencia con el riesgo de la

[45] http://www.privacy-regulation.eu/es/32.htm

[46] Pero, además, será necesario disponer de una evaluación de los riesgos (sistema de análisis de riesgos), lo que en la práctica conlleva diagnosticar distintas variables, como son la probabilidad y gravedad de eventos adversos que puedan afectar a los derechos y libertades de las personas físicas.

actividad u operativa que se encomienda o realiza). De igual modo, corresponderá a ellos la acreditación de medidas adoptadas[47].

6.4. En síntesis, uso de drones y compliance.

Conforme a todo lo expuesto, cabe afirmar que ambos operadores quedan obligados al cumplimiento de la legislación vigente, si bien, se deberá concretar en cada supuesto su competencia y responsabilidad, para lo cual podrá ser necesario examinar el vínculo jurídico o instrumento contractual existente. Esto es, serán responsables del dispositivo, tanto el Responsable del tratamiento de los datos obtenidos, como asimismo la figura del Encargado del mismo, y que actúa bajo la dirección del primero, también ha de asumir la responsabilidad que conlleva su actividad. Así pues, ambos quedan obligados a establecer los sistemas y medidas adecuadas, técnicas y organizativas, coherentes con el grado de impacto y el previo análisis de riesgos evaluado, según el uso y finalidad dado. De igual modo, han de ser adoptadas aquellas medidas óptimas de gestión y ciberseguridad para enfrentar posibles eventos adversos, o amenazas que pudieran afectar al control necesario que se exige (al disponer de información/datos y registrarla). Por tanto, cabe la existencia de supuestos de co-responsabilidad, no obstante el grado puede ser bien distinto.

Ahora bien, por lo general, en el empleo de drones, el operador es el encargado del tratamiento, realizando una actividad conforme al mandato y por cuenta del Responsable del tratamiento, que es el que determina el objeto y ámbito de dicho uso; ordenando su concreta ejecución y prestaciones; o, por ejemplo, vía contrato de arrendamiento de servicios. Por lo que el operador del dron prestará un servicio durante el tiempo pactado, ejecutando su actividad conforme lo preestablecido y acordado, y en atención a lo demandado por el cliente que contrata sus servicios técnicos o profesionales. Al respecto, cabe señalar que ya la Ley 18/2014, de 15 octubre, en su art. 50.1 (2º ap.) estableció un régimen de responsabilidad relativo al operador responsable de una aeronave, siendo *el responsable de la operación,* y como tal deberá asegurar el cumplimiento de toda la legislación vigente, entre otra, la relativa "*la protección de datos o la toma de imágenes aéreas*".

A su vez, obsérvese los deberes que corresponden al Encargado del tratamiento datos, artículo 28 del RGPD. Por tanto, es importante tener en cuenta la posible relación contractual que medie entre ambos sujetos operadores, v.gr., Encargado (operador que ejecuta el servicio, navegación del dron) y Cliente (Responsable que contrata dicho servicio), por lo respecta al cumplimiento legal, régimen previsto por el RGPD. Y, en este sentido, convendrá examinar el clausulado del contrato, de naturaleza civil o mercantil, en lo estipulado para la prestación del servicio/s, así como el posible régimen de garantías (al respecto, cf., artículo 28.3. RGPD).

7. REFLEXIÓN FINAL.

La tutela del derecho a la protección de datos adquiere especial relevancia en el contexto actual y futuro de la Unión Europea, tal y como en los últimos años ya había sido advertido tanto por la doctrina científica como por la jurisprudencia. Ello ha impulsado una significativa evolución de la normativa en esta materia, estableciendo un marco regulatorio básico, común y vinculante en el ámbito de la Unión Europea: el vigente Reglamento General de Protección de Datos (RGPD, 2016), cuyas principales aportaciones han sido expuestas en este estudio.

[47] En lo relativo a la evaluación de los niveles de seguridad y su adecuación, en cada caso deben ser estimados, en congruencia con el previo análisis de riesgos. Por ende, conforme a cada tipología de riesgos, se procederá a su prevención, y se determinará el oportuno tratamiento a seguir, a su vez con base a las distintas categorías (y grado de sensibilidad) de los datos obtenidos. Entre otros riesgos eventuales, también deben ser considerados los relativos a la posible pérdida, destrucción, pérdida o alteración de los mismos, ya fuera por negligencia o intencionada. Por tanto, la atribución de responsabilidad asimismo abarcaría aquellos supuestos accidentales que afectaran a datos personales comunicados, transmitidos, depositados o registrados, esto es, cualquiera que fuese el tratamiento empleado, así como por su comunicación o acceso no autorizados.

Conforme a dicho RGPD, en España, ha sido promulgada la nueva *Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales* (Ley 3/2018, de 5 de diciembre). Esta Ley, constituye un destacado hito jurídico, ya que además de desarrollar el régimen jurídico fijado por el precitado RGPD, lo complementa; e incorpora un Título X "*Garantías de los derechos digitales*", en el que se declara un innovador catálogo de derechos digitales, que, en todo caso, precisaran de posterior desarrollo.

No obstante, aún quedan por resolver cuestiones de interés en esta materia. Pues, hay que reconocer el progresivo incremento de servicios digitales y el empleo de nuevas herramientas o aparatos cada vez más accesibles para la ciudadanía, como acontece en el caso de los drones. Cuyo uso civil o recreativo (inclusive, como "juguete") implica riesgos relevantes, en tanto puede afectar o vulnerar derechos y libertades fundamentales, como son la privacidad y la protección de datos. Por tanto, al respecto, resulta aplicable la citada legislación vigente en materia de protección de datos, y además será necesario reforzar las medidas de supervisión y control, por parte de las autoridades competentes nacionales y europeas.

8. REFERENCIAS BIBLIOGRÁFICAS Y DOCUMENTACIÓN

AA.VV., "El cambio digital en la economía. Un proceso disruptivo*"*. Revista *Información Comercial Española (ICE,)* núm. Núm. 897, julio-agosto 2017. ICE. Secretaría de Estado de Comercio, MINISTERIO DE ECONOMÍA, INDUSTRIA Y COMPETITIVIDAD

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, AEPD (2018). "Guía del Reglamento General de Protección de Datos para responsables de tratamiento". Madrid 2018. Disponible en: https://www.aepd.es/media/guias/guia-rgpd-para-responsables-de-tratamiento.pdf (Fecha última consulta: 10/06/2018).

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, AEPD (2018), "Aprobada la nueva Ley Orgánica de Protección de Datos". Disponible en: https://www.aepd.es/prensa/2018-11-23.html (Fecha última consulta: 28/11/2018).

AEPD, Gabinete Jurídico, Informes jurídicos. Informe RGPD y Drones. Texto disponible en: https://www.aepd.es/media/informes/informe-juridico-rgpd-drones.pdf; y https://www.aepd.es/media/informes/informe-juridico-rgpd-camaras-on-board.pdf

AEPD,"Las Autoridades europeas de protección de datos aprueban el primer Dictamen conjunto sobre drones", en: http://www.lopdat.es/noticias/las-autoridades-europeas-de-proteccion-de-datos-aprueban-el-primer-dictamen-conjunto-sobre (Fecha última consulta: 09/03/2019).

AEPD - GRUPO DE TRABAJO "PROTECCIÓN DE DATOS" DEL ARTÍCULO 29 (PROTECCIÓN DE DATOS), "Dictamen sobre privacidad y cuestiones de protección de datos relativas a la utilización de drones". Disponible en: https://ec.europa.eu/newsroom/article29/news-overview.cfm).

COMISIÓN EUROPEA - Grupo de Trabajo "Protección de datos" del Artículo 29 "Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679". Adoptadas el 4 de abril de 2017. Revisadas por última vez y adoptadas el 4 de octubre de 2017. D.G. Dirección General de Justicia de la Comisión Europea (Bruselas, 2017). - 17/ES, WP 248 rev.01. Disponible en: https://www.aepd.es/media/criterios/wp248rev01-es.pdf

APARICIO SALOM, J. (2013). *Estudio sobre la Ley Orgánica de Protección de Datos de carácter personal.* Aranzadi, Navarra.

ARENAS RAMIRO, M. (2006). *El derecho fundamental a la protección de datos personales en Europa*, Tirant Lo Blanch, Valencia.

BARNÉS VÁZQUEZ, J. (1998). "El principio de proporcionalidad", *Cuadernos de Derecho Público*, 5, Instituto Nacional de Administración Pública, Madrid.

BARRIO ANDRÉS, M. (2018), *Derecho de los drones*. Wolters Kluwer - Colección: Temas La Ley. Madrid.

BOE (2018). *Código del Derecho al Olvido - BOE.es*.

BORIS DELGADO, B. y FERNÁNDEZ, CARLOS M., "La 9 certificaciones para la transformación digital", *Revista AENOR* nº 340, septiembre 2018. págs.13-19.

CAPODIFERRO CUBERO, D. (2017). "La libertad de información frente a Internet", *Revista de Derecho Político*, nº.100, Monográfico con motivo del XL aniversario de la Constitución Española (I), págs. 701-737.

CARBAJO VASCO, D., "El desarrollo de las criptomonedas y su tributación. Cuestiones y respuestas.". *Blockchein Intelligence*. BI Blockchein Law Institute. Serie Doctrinal nº 1. Madrid, junio de 2018. pp. 3-44.

CARRILLO LÓPEZ, M. (2003). *El derecho a no ser molestado: información y vida privada*. Thomson-Aranzadi, Navarra.

CUATRECASAS (2015), "El Grupo de Trabajo del Artículo 29 se pronuncia sobre el uso de drones", en: https://blog.cuatrecasas.com/propiedad-intelectual/el-grupo-de-trabajo-del-articulo-29-se-pronuncia-sobre-el-uso-de-drones/, publicado el 7 de julio de 2015 (Fecha última consulta: 05/03/2019).

DEL ÁGUILA BARBERO, P., "Los drones no se libran de las nuevas medidas de protección de datos", en https://www.eleconomista.es/legislacion/noticias/9332047/08/18/Los-drones-no-se-libran-de-la-nueva-Proteccion-de-Datos.html (Noticia - Fecha: 15/08/2018).

DI PIZZO CHIACCHIO, A. (2016). "Efectos en la jurisprudencia del Tribunal Supremo de la doctrina sentada en el caso "Google Spain": la interpretación de la responsabilidad de los gestores de motores de búsqueda en la implementación del derecho al olvido digital", en *Revista jurídica de Catalunya*, vol. 115, nº.4, págs. 939-976.

DOPAZO FRAGUÍO, M.P., "La protección de datos en el Derecho europeo: Principales aportaciones doctrinales y marco regulatorio vigente (Novedades del Reglamento General de Protección de Datos)", *Revista Española de Derecho Europeo*, REDE nº 68, Octubre – Diciembre 2018. págs. 113 –148.

FORTES MARTÍN, A., "La disciplina jurídico-administrativa de las operaciones con aeronaves pilotadas por control remoto", *Revista General de Derecho Administrativo*, nº 46, 2017.

GONZÁLEZ BOTIJA, F., *Los drones y el derecho de la Unión Europea*. Atelier, Barcelona, 2018.

GONZÁLEZ BOTIJA, F., "Los drones y la Unión Europea", *Revista española de derecho europeo* (REDE), nº. 65, 2018, pp. 37-71.

GONZÁLEZ-DELEITO DOMÍNGUEZ, N., "Los drones: problemática jurídica", *Actualidad administrativa*, nº 5, 2017. pp.31-40.

GONZÁLEZ PUENTE, C. y GONZÁLEZ BOTIJA, F., "Los drones y los derechos fundamentales en la UE", *Revista Universitaria Europea* (RUE) nº 29. julio-diciembre 2018, pp. 77-114.

GUICHOT, E. (2005). *Datos personales y Administración Pública*. APDCM / Thomson-Civitas, Madrid, pág. 230-233.

HERNÁNDEZ LÓPEZ, J.M. (2013). *El derecho a la protección de datos personales en la doctrina del Tribunal Constitucional.* Aranzadi, Navarra.

HERRRÁN ORTIZ, A.I. (2003). "El derecho a la protección de datos en la sociedad de la información", *Cuadernos Deusto de Derechos Humanos*, nº.26, Universidad de Deusto (Bilbao). Disponible en: http://www.deusto-publicaciones.es/deusto/pdfs/cuadernosdcho/cuadernosdcho26.pdf (Fecha consulta: 30/05/2018).

LÓPEZ PORTAS, M.B. (2015). "La Configuración Jurídica Del Derecho al Olvido en el Derecho Español a tenor de la doctrina del TJUE"*, Revista UnED Facultad de Derecho,* nº.93. Disponible en: http://revistas.uned.es/index.php/derechopolitico/article/view/15140. (Fecha consulta: 30/05/2018).

LOZANO, S. (AENOR), "El Delegado de Protección de Datos, el profesional más buscado", *Revista AENOR* nº 340, septiembre 2018. págs.24-27.

LUCAS MURILLO DE LA CUEVA, P. (2008). "El derecho a la autodeterminación informativa y la protección de datos personales", *Azpilcueta: cuadernos de derecho*, nº.20, págs.43-58.

LUCAS MURILLO DE LA CUEVA, P. (2000). "Las vicisitudes del derecho de la protección de datos personales", en *Revista Vasca de Administración Pública*. Vol. 2, n.º 58, pág. 211-242.

MARTÍNEZ MARTÍNEZ, R. (2007). "El derecho fundamental a la protección de datos: perspectivas", Monográfico «III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas», *Revista de los Estudios de Derecho y Ciencia Política de la UOC*, IDP, nº5, págs.47-61. Disponible en: https://dialnet.unirioja.es/descarga/articulo/2372613.pdf*; y,* https://idp.uoc.edu/articles/10.7238/idp.v0i5.436/galley/3341/download/ (Fecha consulta: 30/05/2018).

NÚÑEZ LÓPEZ, M. y DEL MAR FERREIRO, M. (2013). "Una aproximación para empresas a la Ley Orgánica de Protección de Datos", en *Derecom*, nº. 15. Nueva Época. Septiembre-Noviembre, págs. 93-109. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=4399157 (Fecha consulta: 30/05/2018).

OLLERO TASSARA, A. (2008). *De la protección de la intimidad al poder de control sobre los datos personales. Exigencias jurídico-naturales e historicidad en la jurisprudencia constitucional.* Real Academia de Ciencias Morales y Políticas, Madrid.

ORTI VALLEJO, A. (1994). "El nuevo derecho fundamental (y de la personalidad) a la libertad informática (a propósito de la STC 254/1993, de 20 de julio)", *Derecho Privado y Constitución,* núm. 2. Enero-Abril, págs. 305-332.

PIÑAR MAÑAS, J.L. (Dir.) (2016). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de protección de datos*. Reus, Madrid.

PIÑAR MAÑAS, J.L. (2014). "Aplicación extraterritorial de la Directiva 95/46/CE sobre protección de datos y derecho al olvido frente a los motores de búsqueda. Comentario rápido a la Sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014, Caso GOOGLE", en *Iuris: Actualidad y práctica del derecho*, nº 215, págs. 20-23.

PIÑAR MAÑAS, J.L. (2014). "Transparencia y derecho de acceso a la información pública: algunas reflexiones en torno al derecho de acceso en la Ley 19/2013, de transparencia, acceso a la información y buen gobierno", *Revista catalana de dret públi*c, nº. 49, págs. 1-19.

PIÑAR MAÑAS, J.L. (2008). *"¿Existe la privacidad?",* Universidad CEU San Pablo, Madrid 2008 (págs.10-11 y p. 12). Disponible en: http://dspace.ceu.es/bitstream/10637/3372/1/Lecci%C3%B3n%20Magistral%20Inaug%20%20curso%2008-09%20USP.pdf (Fecha consulta: 02/06/2018).

RALLO LOMBARTE, A., "Protección de datos y derechos digitales", en "Protección de datos, intimidad, libertad", *Registradores de España* nº 84., 2018, p.16.

RALLO LOMBARTE, A. (2017). "De la 'libertad informática' a la constitucionalización de nuevos derechos digitales (1978-2018)", *Revista de Derecho Político*. Monográfico con motivo del XL aniversario de la Constitución Española (I). nº.100, págs. 639-669.

REBOLLO DELGADO, L. (2000). *El derecho fundamental a la intimidad*. Dykinson, Madrid, págs.78 y 79.

REBOLLO DELGADO, L. y SERRANO PÉREZ, Mª. (2014). *Manual de protección de Datos*. Dikynson, Madrid 2014.

RODRIGUEZ, M., GÓMEZ, A.I. y DELGADO, B., "Nueva certificación para el gobierno, gestión y calidad de los datos", *Revista AENOR* nº 340, septiembre 2018. págs.28-33.

RUIZ MIGUEL, C. (1994). *El derecho a la protección de la vida privada en la jurisprudencia del Tribunal Europeo de Derechos Humanos*. Civitas Madrid.

RUIZ MIGUEL, C. (2003). "El derecho a la protección de los datos personales en la Carta de Derechos Fundamentales de la Unión Europea : análisis crítico", *Revista de Derecho Comunitario Europeo*, nº14, págs. 7-43. Texto disponible en: https://dialnet.unirioja.es/servlet/autor?codigo=176117. (Fecha consulta: 30/05/2018).

SARRIÓN ESTEVE, Joaquín, "El régimen jurídico de la utilización de drones en España", ponencia en Seminari de la Facultat de Dret de València, 25 de Mayo de 2016. Working paper disponible en: https://www.uv.es/seminaridret/sesiones2016/drones/ponenciaSarrion2016 (Fecha última consulta: 23/02/2018).

SIMÓN CASTELLANO, P. (2012). *El régimen constitucional del derecho al olvido digital*. Tirant lo Blanch, Valencia, págs. 115 y ss.

SIMÓN CASTELLANO, P. (2012). "El encaje constitucional del derecho al olvido digital en perspectiva comparada", en *Datospersonales.org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, nº. 54.