Congreso Derecho TICs - SICARM 2014: Innovación, tecnología y gestión avanzada de la información administrativa. Implicaciones jurídicas del cambio de paradigma

El uso de vehículos aéreos no tripulados (drones) en las labores de seguridad y vigilancia de la Administración

Protección de la intimidad y responsabilidad de las Administraciones Públicas

MAR ELORDI VILLENA

23-24 Octubre 2014

El avance de la tecnología dron ha aumentado exponencialmente en los últimos años. La posibilidad de que el mecanismo de seguridad y control del Estado alcance el espacio aéreo, activa las alarmas en el ámbito de la privacidad. El uso indiscriminado estas aeronaves puede producir vulneraciones en la esfera de la intimidad de los individuos, sin embargo su uso cotidiano en labores de la Administración parece imparable. Es por ello que se hace necesario adelantarse un paso y preguntarse qué incógnitas planteará el desarrollo de esta tecnología.

En el curso de este último año hemos visto despuntar en todas las portadas noticias sobre unas aeronaves no tripuladas que van a revolucionar el mundo del transporte. Los hay que piensan así, y también los hay que opinan que estos drones traerán el nuevo 1984. Privacidad Vs. Seguridad es probablemente el principal debate de nuestro tiempo. Los drones son sólo una parte de este conjunto de nuevos retos que nos plantea la sociedad de la información, a los que se suman tecnologías como el "big data", o el "internet de las cosas".

Una cosa está clara, los drones son la siguiente generación de sistemas de transporte. Es el medio menos costoso, el más rentable energéticamente, el más ecológico, el más versátil y fácil de implementar que existe en el mundo. Un sistema que funciona en cualquier territorio y en los climas más extremos; que conecta a cualquier persona en cualquier lugar.

Sólo en la Unión Europea hay más de 5 millones de kilómetros de carretera, una infraestructura de costosa construcción y mantenimiento, que tiene una huella ecológica devastadora. ¿Es posible hacerlo mejor? ¿Es posible eliminar las barreras espaciales, como hizo internet con la barrera temporal? Muchos países tienen excelentes redes de telecomunicaciones sin haber tenido que instalar un solo cable de cobre ¿Se puede hacer lo mismo con el transporte? La principal ventaja de los drones es que no necesitan una estructura física. Los drones vuelan allí donde haya aire, y las carreteras en el aire sólo requieren una autorización. Es una infraestructura desmaterializada, únicamente de software.

Analicemos la siguiente perspectiva: La mitad de la población mundial vive en ciudades, medio millón en megaciudades. Vivimos una tendencia a la superpoblación. Únicamente en China surge una ciudad del tamaño de Nueva York cada dos años. En estos lugares, la ineficiencia de la infraestructura genera un enorme problema de congestión en la circulación; y va en aumento. Para solucionar este ineludible problema tendría sentido una red de transporte que se sitúe en una capa intermedia, a caballo entre internet y las carreteras. Una red que resuelva las dificultades del envío urgente, transporte ligero y rápido. Una solución moderna para un conflicto muy antiguo. Un sistema con una alta escalabilidad y una muy baja huella ecológica, que operase en un rango horario de 24 horas 7 días a la semana, al igual que lo hace internet.

Un estudio publicado por la Asociación Internacional de Sistemas Aéreos no Tripulados (AUVSI) prevé que si la Administración Federal de Aviación estadounidense cumple con la fecha límite para la integración en el espacio aéreo civil de estas aeronaves no tripuladas (UAS) en 2015, el total de Impacto Económico llegará a 82,1 billones de dólares entre 2015 y 2025. Además, se crearán más de 100.000 empleos de alta remuneración en el proceso de integración (sin contar los que se generarán con el desarrollo de esta industria).

Lo cierto es que estamos siendo testigos del comienzo de una era en la que estos robots no tripulados van a cambiar el mundo y la forma en que vivimos en él. Esto, no obstante, es sólo el comienzo; se está gestando un nuevo paradigma para el transporte: una red de sistemas aéreos no tripulados que actúe de forma interconectada para dar respuestas ágiles y precisas. Asistimos al acortamiento de las

distancias, la eliminación definitiva de las barreras espaciales. A quienes aún crean que esto es ciencia ficción, les digo firmemente que no lo es: los drones son para el transporte lo que la telefonía móvil para las telecomunicaciones.

Desgraciadamente no todo es un camino de rosas para el desarrollo de esta tecnología. La utilización de drones entraña serios conflictos en el ámbito de la privacidad de los ciudadanos; especialmente si se aplica en el campo de la seguridad y vigilancia. A continuación trataremos las consecuencias de su uso por la Administración, para ello, esta exposición se divide en dos partes correspondientes a las dos grandes incógnitas que aquí se plantean.

La primera de ellas trata de la problemática en materia de protección de datos, en qué casos se debilita este derecho y en qué puntos hay un desajuste normativo que permite intromisiones ilegítimas en la esfera de la intimidad. La segunda parte hace referencia a la responsabilidad de la Administración a consecuencia de la introducción de drones en los servicios públicos, fundamentalmente nos preguntaremos cuándo son imputables a la Administración los daños causados a particulares y por tanto cuándo existe deber de indemnizar. Pero en primer lugar se analizará brevemente qué son estas aeronaves no tripuladas y cuáles son sus principales funcionalidades.

¿Qué es un dron?

Un dron es una aeronave no tripulada pilotada por control remoto, también se conocen por sus siglas en inglés como RPAS (Remotely Piloted Aircraft Systems) o UAV (Unmanned Air Vehicle). La definición jurídica en España la encontramos en el recién modificado Real Decreto 1489/1994, de 1 de julio, por el que se aprueba el Reglamento de la Circulación Aérea Operativa, que dice así:

> *Vehículo aéreo no tripulado: Vehículo aéreo propulsado que no lleva personal como operador a bordo. Los vehículos aéreos no tripulados (UAV) incluyen solo aquellos vehículos controlables en los tres ejes. Además, un UAV:*
>
> *a) Es capaz de mantenerse en vuelo por medios aerodinámicos.*
>
> *b) Es pilotado de forma remota o incluye un programa de vuelo automático.*
>
> *c) Es reutilizable.*
>
> *d) No está clasificado como un arma guiada o un dispositivo similar de un solo uso diseñado para el lanzamiento de armas.*

El amplio abanico de funciones que ofrecen estas aeronaves permite distinguir cuatro grandes campos en función del colectivo que los utilice:

- Uso militar
- Uso privado
- Uso en servicios públicos
- Uso civil o drones de recreo

Actualmente en España el uso de drones está prohibido, por un comunicado que emitió la Agencia de Seguridad Aérea Española, que sentenciaba: "*no está permitido, y nunca lo ha estado, el uso de aeronaves pilotadas por control remoto con fines comerciales o profesionales para realizar actividades consideradas trabajos aéreos, como la fotogrametría, agricultura inteligente, reportajes gráficos de todo tipo, inspección de líneas de alta tensión, ferroviarias, vigilancia de fronteras, detección de incendios forestales, reconocimiento de los lugares afectados por catástrofes naturales para dirigir las ayudas adecuadamente, etc.*"

La expansión del mercado de los drones se ve inhibida por la ausencia de un marco reglamentario adecuado en la Unión Europea, y por la necesidad de obtener una autorización individual de cada Estado en el que los fabricantes y proveedores quieran entrar. Algunos Estados han comenzado a legislar para facilitar este proceso de autorización, pero a falta de las normas europeas que debe elaborar la EASA (Agencia Europea de Seguridad Aérea), no surgirá un verdadero mercado europeo, lo que obstaculizará de forma drástica la expansión de este sector. Asimismo para algunas clases de operaciones de UAV hace falta un mayor progreso en la tecnología instrumental adecuada. Por otro lado, el desarrollo de aplicaciones no militares exige un marco garantista para que no suponga una amenaza a la privacidad o integridad física de los ciudadanos. Todas las miradas están puestas en la regulación de los drones, la industria retrasa las inversiones hasta que el marco legal ofrezca la suficiente seguridad jurídica.

Uso de drones por las Administraciones Públicas: problemática sobre protección de datos

Esta tecnología está empezando a avanzar, y ya se han dado algunos casos en los que los drones han supuesto un problema para el derecho a la privacidad. El más sonado y reciente es la captación de imágenes que realizó un dron de las futuras instalaciones de Apple, un macroedificio que se hace llamar "nave espacial". Este proyecto, el último que presentó en público Steve Jobs, se ha llevado desde entonces con extremo secreto. Pues bien, en agosto de 2014 un anónimo "youtuber" elevó un dron por encima de estas instalaciones tirando por tierra todo secreto y mostrando abiertamente lo que tanto se había preocupado Apple por proteger. Pero este no es el único caso, ni el más alarmante.

En junio del mismo año, una chica de Seattle estaba en su apartamento (un piso 26) cuando observó que un dron revoloteaba cerca de su ventana captando imágenes del edificio. La joven denunció los hechos a la policía quien localizó al dueño del dron. La empresa propietaria del UAV afirmó haber tomado fotografías de la fachada para trabajos con arquitectos, promotoras e inmobiliarias. Un asunto cuanto menos intrigante.

Estos casos han sido los primeros de una previsible lista de intromisiones en el ámbito privado de los particulares. En este orden de cosas surgen preguntas como ¿Es suficiente una regulación basada en la normativa sobre tráfico aéreo? ¿En qué puntos se vulnera el derecho de protección de datos? ¿Es equiparable el régimen de autorizaciones y normas sobre videovigilancia? La regulación en el ámbito de la

seguridad aérea es otro factor en el que aquí no se profundizará para acotar el discurso.

En relación con las labores llevadas a cabo por drones en servicios públicos, la normativa que resulta de aplicación es la LO 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos, y su Reglamento de desarrollo (Real Decreto 596/1999, de 16 de abril). Sin embargo, es preciso analizar la modulación de los principios de protección de datos y de videovigilancia en estos casos de uso de drones. Más adelante se profundizará concretamente los puntos referidos al derecho de información y a las autorizaciones (distinguiendo éstas últimas de las eventuales autorizaciones en materia de aviación).

Principios de protección de datos y videovigilancia

La normativa sobre protección de datos protege los principios de información en la recogida de datos, calidad de los mismos, finalidad en el tratamiento, consentimiento en la recogida de datos y seguridad; y están plasmados en diversos preceptos de la LOPD. De manera específica, la normativa sobre de videovigilancia establece los principios de idoneidad, intervención mínima y peligro concreto, previstos en el artículo 6 de la LO 4/1997. Para que la incorporación de UAVs en servicios públicos cumpla con las exigencias de privacidad impuestas por estos principios, hace falta ser cauto en determinadas aplicaciones para no sobrepasar la delgada línea entre la seguridad y los derechos individuales de los particulares.

El principio de idoneidad hace referencia a la adecuación del medio a la situación concreta, que en todo caso ha de tratarse de un peligro para la seguridad ciudadana. Sería cuestionable entonces el uso de drones para controlar las fronteras o en los ámbitos agrario y medioambiental. No obstante, podría ser un medio adecuado, la vigilancia mediante sensores térmicos (en lugar de imágenes) para el seguimiento de cultivos o poblaciones animales.

El principio de intervención mínima resulta de la ponderación entre la finalidad pretendida y el grado de afectación a la esfera de privacidad. El especial valor que tiene la grabación por medio de drones es su amplio campo de visión y la claridad y nitidez de las imágenes. Es por ello que, a pesar de que se establezca una limitación en el área de filmación, es muy probable que el UAV capte imágenes del interior de los edificios de su alrededor; por tanto, hay que considerar que cuanto mayor sea la limitación de la esfera de intimidad, más importantes deberán ser los intereses generales que se persigan. Existen mecanismos de mitigación del riesgo, como determinados programas de anonimización de vídeo, que analizan las imágenes y cuando captan una cara humana, destruyen automáticamente el fotograma (La AEPD considera válido este mecanismo en la investigación sobre Google Street View, E/01829/2012).

El peligro concreto cristaliza así en la SAP de Bilbao de 10 de enero de 1995 (entre otras): "*la instalación de las cámaras videográficas tenía una finalidad de prevención del delito y de garantía de la seguridad pública. Era, y es, un hecho notorio, incluso publicado, que en esa fecha, concretamente, como había sucedido en años anteriores, se iban a producir alteraciones del orden público, con motivo del izado de la bandera*

española, en el Ayuntamiento de Bilbao". Estaría entonces justificado el uso de drones en manifestaciones y aglomeraciones o eventos donde el peligro fuese previsible (sin perjuicio de las medidas para evitar daños de una posible caída del dron).

Finalmente, han de ser destruidos los datos obtenidos en el interior de viviendas, o cuando afecte directamente a la intimidad aunque se trate de lugares públicos, incluyendo las conversaciones privadas. En la STC 98/2000, de 10 de abril el Tribunal señaló que, *la captación de audio desborda el principio de proporcionalidad considerando que es una intromisión ilegítima en el derecho a la intimidad, al no quedar acreditado que el uso de micrófonos, que permitía la audición continuada e indiscriminada de todo tipo de conversaciones […] resultase indispensable para la seguridad y buen funcionamiento del establecimiento*. Por lo que la instalación de dispositivos de audio en los drones debería estar restringida. Este precepto da un margen a la posible captación de imágenes de la esfera de la intimidad, ya que prevé su eliminación. Es decir, siempre que el dron grabe imágenes de este tipo, deberán ser borradas por no cumplir con los principios de protección de datos y de vigilancia. Pero este margen de error debe reducirse en caso de la utilización de UAVs, pues el perjuicio aparejado es exponencialmente superior. Si no se toman las precauciones necesarias para reducir este margen de error un "hacker" además de controlar la trayectoria del dron podría acceder a los datos que en él se almacenasen.

Derecho de información

El artículo 9 de la LO 4/1997, consagra un deber derivado del derecho de información de la recogida de datos del artículo 5 de la LOPD. Obliga a informar al público de la existencia de videocámaras y de la posibilidad de ejercitar sus derechos ARCO ante el responsable del fichero. Este deber de información no plantea problema alguno en espacios públicos acotados. Un estadio o un recinto ferial al aire libre constituyen espacios delimitados en los que se puede cumplir esta obligación si se coloca el cartel informativo en los accesos, ya sean espacios abiertos o cerrados.

Sin embargo, los UAV ofrecen nuevas posibilidades y nuevas aplicaciones, entre ellas, la de controlar manifestaciones o eventos públicos importantes, vigilar las fronteras, etc. En estos casos el dron se mueve por una zona no acotada y por tanto el deber de información deviene irrealizable. Pongamos por caso un gran evento en Madrid, una visita del Papa, se elevarían drones por toda la ciudad siendo imposible colocar letreros en cada esquina ¿decaería entonces del derecho de información a favor de un bien jurídico superior, la seguridad? En principio sí podríamos ver como la ponderación de intereses se inclina hacia la seguridad. Sin embargo también podrían contemplarse mecanismos alternativos de información como su publicación en periódicos o informativos.

Es necesario traer a colación el caso del ayuntamiento de Madrid que ya opera en prácticas con un UAV en el proyecto piloto SOS Drone para apoyo de los servicios de Bomberos, Samur y Policía municipal. El dron fue empleado por primera vez en septiembre de 2013, cuando los madrileños se concentraron en la Puerta de Alcalá para conocer si Madrid sería ciudad olímpica. Resulta sorprendente y alentador que la tecnología dron avance a este ritmo, pero ¿la normativa de protección de datos fue respetada? La respuesta es no. Lo que no resulta nada alentador sino más bien

inquietante es que el Ayuntamiento prevé redactar a finales de este año un contrato para la utilización del dron por personal municipal los 365 días del año. Esperemos que también prevea acatar las cautelas necesarias en materia de protección de datos.

Autorizaciones

Existen dos regímenes de autorizaciones aplicables. De un lado las autorizaciones en materia de aviación, que en un primer avance normativo, ya son contempladas por el Real Decreto-ley 8/2014, de 4 de julio, de aprobación de medidas urgentes para el crecimiento, la competitividad y la eficiencia en su Sección 6, pero que no se analizarán en profundidad por exceder de los límites de esta exposición. De otro lado, el régimen de autorizaciones contemplado en la LO 4/1997 hace referencia a los permisos administrativos necesarios para poner en funcionamiento videocámaras en lugares públicos.

Los artículos 3 y 5 establecen las pautas sobre autorizaciones de videocámaras fijas y móviles. Continuando el procedimiento de análisis que hemos seguido hasta ahora, es importante distinguir tres eventuales situaciones, en concurrencia con drones, para comprobar si el precepto se ajusta a las exigencias de estos UAVs.

- *Sustitución de cámaras móviles por drones*: existiendo ya autorización para la instalación de una cámara móvil ¿este permiso sería suficiente para abarcar la actividad de un UAV? Aquí se vuelve a plantear la dificultad de la delimitación del espacio, mientras que para una cámara móvil es fácil, para un dron no lo es. Piénsese en un dron que hace rondas en torno a un edificio público en mitad de Madrid. Dado su amplio campo de visión, sería complicado evitar la captación de imágenes de la vía pública e incluso del interior de los edificios cercanos.
- *Incorporación de drones existiendo cámaras fijas*: Cabe pensar que la autorización para las cámaras fijas no sería suficiente, habría que solicitar además una autorización para videocámaras móviles o drones. También en este punto nos encontramos con el problema de la *sobrevigilancia*. En unas instalaciones en las que ya existen cámaras fijas, la suma de drones a las tareas de vigilancia podría suponer una carga excesiva para los trabajadores que se encuentren todo el tiempo “controlados”.
- *Aplicación de drones sin existir autorización previa de ningún tipo*: Este caso está excluido de la aplicación del precepto, ya que no existe una autorización específica para estos UAVs. Cabría preguntarse si estas aeronaves no tripuladas encajan en el concepto de videocámara móvil que da la norma, o por el contrario es necesaria una previsión específica.

Uso de drones por las Administraciones Públicas: responsabilidad de la Administración

Otra gran controversia que plantea el uso de drones en servicios públicos es la responsabilidad de la Administración. Los artículos 106.2 y 149.1.18º CE[1], el Título X de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, y el Real Decreto 429/1993, de 26 de marzo, por el que se aprueba el Reglamento de los Procedimientos de las Administraciones Públicas en materia de responsabilidad patrimonial; establecen el marco jurídico aplicable. La Administración tiene un margen de responsabilidad más amplio que el de los particulares, el cual sirve de garantía del buen funcionamiento de los servicios públicos, y pivota en torno a tres principios fundamentales:

- **Responsabilidad total**: esta responsabilidad se aplica tanto a las Administraciones de Derecho público, AGPD, como a las de Derecho privado; por ejemplo una sociedad mercantil encargada del salvamento marítimo como puede ser Remolques Marítimos S.A., participada al 100% por el Estado Español.
- **Responsabilidad directa**: ha de exigirse directamente a la Administración ya que no es subsidiaria de sus agentes. Si se ejerce una acción de responsabilidad contra un miembro del cuerpo de policía que controla un dron, habría causa de una excepción por falta de legitimación pasiva. Ello sin perjuicio de que la Administración esté obligada a repetir contra el agente que causó el perjuicio.
- **Responsabilidad objetiva**: la Administración responde con independencia del funcionamiento normal o anormal del servicio. Habría responsabilidad por la caída de un dron a causa de una ráfaga de viento; pero también si un funcionario lo utiliza para tareas personales.

Dado su carácter garantista, la responsabilidad extracontractual de la Administración dibuja una esfera más amplia que la contemplada en los artículos 1902 y *ss* del Código Civil. A la hora de introducir los drones en la prestación de servicios públicos, es preciso examinar ciertas zonas de penumbra en las que no es fácil distinguir este margen de responsabilidad. Como se ha visto, los drones pueden integrarse en multitud de actividades de la Administración, como el control del tráfico o las fronteras, las acciones de socorro y salvamento, la seguridad ciudadana en general, etc. Haciendo una predicción las eventuales lesiones que se puedan derivar, se diferencian dos tipos de responsabilidad:

- Responsabilidad por daños materiales: tanto a personas (lesiones corporales) como a cosas. El ejemplo más obvio es la responsabilidad derivada de la caía de un dron.
- Responsabilidad por intromisión en el ámbito de la privacidad: por lesión de los derechos a la intimidad personal y familiar y a la protección de datos personales.

[1] Esta responsabilidad, es consagrada en nuestra Constitución cuyo artículo 106.2 de reza así: *Los particulares, en los términos establecidos por la ley, tendrán derecho a ser indemnizados por toda lesión que sufran en cualquiera de sus bienes y derechos, salvo en los casos de fuerza mayor, siempre que la lesión sea consecuencia del funcionamiento de los servicios públicos.*

La problemática que despierta la introducción de los drones en la vida administrativa puede resumirse en tres grandes cuestiones, que se analizan a continuación: (i) ¿Hay responsabilidad por la identificación de personas y utilización de sus datos?; (ii) ¿Cómo se modula el sistema de responsabilidad cuando interviene un tercero?; (iii) ¿Es imputable la acción dañosa a un individuo concreto?

(i) Identificación de personas

Al hablar de la compatibilidad entre la privacidad y los drones, se han visto previamente posibles actuaciones que rebasan un uso correcto de los mismos. Un ejemplo ilustrativo puede ser el del control del tráfico: si el dron capta la matrícula del vehículo infractor para imponerle una sanción, no existe peligro alguno de violación de la privacidad, ya que es un acto justificado. Pero qué pasaría si el dron almacena en una lista matrículas recurrentemente infractoras, y se dedica a "perseguir" a estos vehículos, en aras de imponer una sanción. Bajo la apariencia de una medida para aumentar el nivel de seguridad vial, se puede apreciar una vulneración de la esfera de privacidad de los ciudadanos. ¿Estaría este acto, la identificación y posterior persecución, justificado por la protección de un bien común?

A este respecto, la jurisprudencia administrativa aplica la teoría del "deber de soportar el daño" previsto en el artículo 141.1 LRJPAC. Se ha tratado de suplir la vaguedad de este concepto aplicando un parámetro objetivo que, todo sea dicho, también dista de ser concreto, así hablamos del "estándar de seguridad exigible". Según este criterio, el daño será antijurídico sólo cuando la actividad administrativa sobrepase los límites de seguridad exigibles.

La STS (Sala 3ª), de 21 de diciembre de 1998, recoge el supuesto de una manifestación ilegal en la que se procede a su disolución mediante el empleo de un chorro de agua a presión, que produce el desprendimiento de retina de uno de los manifestantes. El TS declara que éste tiene el deber de soportar el daño pues su conducta ilegal justifica la actuación de la policía y por tanto no es antijurídica[2]. En otras sentencias, como en la STS de 10 de abril de 2000 también se falla en este sentido "*Y esto es lo que aquí ocurre. Pues es patente que la profesión de piloto militar es una profesión de alto riesgo, hasta el punto de que, incluso las misiones de entrenamiento pueden tener un elevadísimo componente de peligrosidad, como ocurre con la encomendada al capitán don R.S.S"* [3] En este caso es la peligrosidad la que justifica la lesión.

[2] La STS (Sala 3ª), de 29 de octubre de 1998, así lo afirma con toda claridad: <*debe, pues, concluirse que para que el daño concreto producido por el funcionamiento del servicio a uno o varios particulares sea antijurídico basta con que el riesgo inherente a su utilización haya rebasado los límites impuestos por los estándares de seguridad exigibles conforme a la conciencia social. No existirá entonces deber alguno del perjudicado de soportar el menoscabo y, consiguientemente, la obligación de resarcir el daño o perjuicio causado por la actividad administrativa será a ella imputable*> (F. J. 4.º).

[3] STS de 10 de abril de 2000, FJ 3º *: Nuestra Sala tiene dicho -S. de 10 de octubre de 1997- que «el punto clave para la exigencia de la responsabilidad no está en la condición normal o anormal del actuar administrativo, sino en la lesión antijurídica sufrida por el afectado y que éste no tiene el deber jurídico de soportar, por lo que la antijuricidad desaparece cuando concurre una causa justificativa que legitime el perjuicio, "un título que imponga al administrado la obligación de soportar la carga" -S. de 3 de enero de 1997, Ar. 7-- "o algún precepto legal que, imponga al perjudicado el deber de sacrificarse por la sociedad" - S. de 27 de septiembre de 1997, Ar. 3299». Y esto es lo que*

La respuesta a la cuestión de la identificación de personas dependerá entonces de si esta utilización de los datos está justificada. La dificultad está en dibujar la línea entre quién tiene el deber de soportar el daño y en qué circunstancias concretas de la actuación de estos drones decae el derecho de privacidad.

(ii) intervención de un tercero

La intervención de un tercero en la actividad del dron puede causar serios perjuicios tanto a la Administración como a los particulares. Las dos situaciones más ilustrativas son las de derribo y hackeo del dron. Representa un peligro para una multitud, por ejemplo, en una manifestación que un dron sobrevuele el tumulto. Un UAV de tamaño medio tiene un peso de 5 a 10 kilos, teniendo en cuenta también la altura si cayese sobre una persona le causaría graves lesiones e incluso la muerte. Aunque no aparentemente, el hackeo de un dron puede causar perjuicios similares o incluso mayores. El dron es un robot que posee un sistema informático a modo de "cerebro", en él están las órdenes que determinan su actuación. Téngase en cuenta toda la información que se almacena en un dron, un hacker no sólo tendría acceso a toda esa información, sino que podría inducir al dron a que "atacase" a una persona. El sistema de seguridad informática nacional debe jugar en este punto una posición fuerte, vistos los potenciales riesgos del uso de drones.

¿Cuál es el papel de la Administración en esta situación? La teoría de la responsabilidad patrimonial de las Administraciones Públicas declara que no es suficiente que el servicio público se inserte en la relación de causalidad. Para que la Administración indemnice tiene que haber una relación directa entre la actuación de la Administración y la producción del resultado. ¿Podemos entonces decir que si un dron es hackeado respondería la Administración?

Al echar un vistazo a la jurisprudencia la STS de 25 de enero de 1997, establece una modulación en esta relación de causalidad "*la imprescindible relación de causalidad entre la actuación de la Administración y* ***el resultado dañoso producido puede aparecer bajo formas mediatas, indirectas y concurrentes*** *(aunque admitiendo la posibilidad de una moderación de la responsabilidad en el caso de que intervengan otras causas, la cual debe tenerse en cuenta en el momento de fijarse la indemnización).*". En esta línea la STS de 28 de marzo de 2000 afirma que "***No es obstáculo a la existencia de responsabilidad patrimonial*** *de la Administración en los casos de fallecimientos de internos en establecimientos penitenciarios por obra de otra persona -o, en el caso que examinamos, por su propia voluntad suicida-* ***el carácter directo, inmediato y exclusivo con que la jurisprudencia viene caracterizando el nexo causal entre la actividad administrativa y el daño o lesión***"

(iii) Imputabilidad del daño

Aquí se habla de la responsabilidad del tercero agente de la Administración pero es importante precisar que se está haciendo referencia a la responsabilidad última, es

aquí ocurre. Pues es patente que la profesión de piloto militar es una profesión de alto riesgo, hasta el punto de que, incluso las misiones de entrenamiento pueden tener un elevadísimo componente de peligrosidad, como ocurre con la encomendada al capitán don R.S.S.

decir, al agente que causa el daño. Como se ha dicho anteriormente, la responsabilidad de la Administración es directa, por tanto nos estaremos refiriendo al deber de la Administración de repetir contra el causante del daño.

Para establecer un criterio sobre la responsabilidad de la Administración, primero hay que examinar la relación entre el dron y la persona que lo controla, ya sea por control remoto, ya sea automatizándolo. El primero de los casos parece claro, el funcionario que esté controlando el dron a tiempo real es el responsable del daño de forma análoga a como sucedería si controlase una excavadora, por ejemplo. En resumen, cuando el dron actúa por control remoto, puede ser considerado como una herramienta al servicio de la Administración, por lo que la causalidad acto-lesión es directa.

Una situación jurídica algo difusa es la de la programación de un dron para que realice actividades de manera autónoma. ¿Qué papel juega el programador? ¿Es responsable indirecto? Si ha habido un fallo de programación imputable a esta persona, parece razonable pensar que sí cabría la repetición. Pero ¿y si ha cumplido con las pautas de programación asignadas y aún así se produce la lesión?

La responsabilidad por riesgo o funcionamiento normal de los servicios públicos cubre los supuestos de caso fortuito, pero excluye los supuestos de fuerza mayor. El artículo 139.1 de la Ley 30/92 así lo afirma "*Los particulares tendrán derecho a ser indemnizados por las Administraciones Públicas correspondientes, de toda lesión que sufran en cualquiera de sus bienes y derechos, salvo en los casos de fuerza mayor, siempre que la lesión sea consecuencia del funcionamiento normal o anormal de los servicios públicos*."

El caso fortuito comprende los daños causados por hechos imprevisibles o inevitables, pero producidos dentro de la prestación del servicio público o de la organización administrativa (ej. el fallo imprevisible del software que produce la caída y consecuentes daños materiales en un tejado). Por otro lado, la fuerza mayor se refiere a hechos imprevisibles o irresistibles, ajenos por completo a la actividad administrativa (ej. Fuerte viento que desvía la trayectoria del dron resultando una colisión).

No obstante el artículo 141.1 LRJPAC establece límites a la indemnización de daños imputables a caso fortuito al excluir la responsabilidad por daños imprevisibles e inevitables conforme al estado de la ciencia y de la técnica. De esta manera, el legislador establece un estándar de diligencia en aquellos ámbitos en los que se siga un criterio de actuación científico o técnico. Es decir, si se producen daños que se pudieron prever y evitar conforme a los conocimientos científicos o técnicos actuales, la Administración no responderá. En resumen, en ámbitos de actuación administrativa guiadas por la ciencia y la técnica existe una limitación del alcance de la responsabilidad objetiva, mediante la restricción de la imputación de daños, al criterio de la culpa.

Conforme a lo expuesto, en este concreto ámbito (la utilización de drones) la responsabilidad de la Administración sólo surgiría en caso de funcionamiento anormal del servicio, es decir de culpa. Esta doctrina se queda coja si tenemos en cuenta las múltiples capacidades y la alta versatilidad de los UAVs. A continuación se expone un

posible futuro caso que plantea controversias más allá de lo dispuesto en las normas que existen hasta ahora.

> *Un ayuntamiento que ofrece un servicio de filmación del estado de las playas en streaming utiliza un dron que capta panorámicas en las que no se identifican personas, y por tanto se excluye de la obligación de avisar que es una zona videovigilada. Sin embargo un barco de recreo se coloca cerca del dron de manera que se pueden identificar a los tripulantes y, accediendo a la página web de dicho ayuntamiento, se puede ver todo lo que estas personas hacen*.

La doctrina se pronuncia hasta un punto en el que se han podido resolver las cuestiones jurídicas planteadas, pero será insuficiente cuando convivamos con drones que controlan el tráfico o patrullan los bosques. La introducción de estas aeronaves no tripuladas en los quehaceres de la Administración abre la puerta a nuevas incógnitas aún sin resolver.

Los drones forman parte de una tecnología muy avanzada, que brinda nuevas técnicas y funcionalidades, es por ello que la norma no está completamente adaptada. En cuanto a las colisiones con los principios de protección de datos, es posible respetar la esfera de la intimidad con la utilización de estas nuevas técnicas como sensores térmicos, auto-eliminación de fotogramas, etc. Sin embargo, los regímenes de información y de autorizaciones se hallan completamente desconectados de esta tecnología. Lo mismo sucede con la responsabilidad de la Administración, especialmente ante situaciones de drones autónomos que pueden producir perjuicios sin que sea posible identificar a una persona culpable. Los UAVs tienen intención de venir para quedarse, pero ello no obsta a que las autoridades responsables prevean una adaptación del ordenamiento para un uso fiable de los mismos.

Fundamentalmente, esta red está diseñada en torno a la necesidad humana, y sin las limitaciones que entraña la arcaica tecnología de las redes de transporte actuales. Cuando surge una necesidad, por ejemplo en el caso de un escalador extraviado, hoy en día lo primero sería llamar a los servicios de emergencia y salvamento que activarán la respuesta de socorro. Esta es la parte que funciona. Sin embargo la ayuda puede tardar días en llegar por la inaccesibilidad del lugar. Esta es la parte que hay que arreglar. Es necesaria una red logística flexible y automatizada. Dado que actualmente somos capaces de detectar el problema a la velocidad de internet, es de esperar que seamos capaces de solucionar dicho problema a la velocidad de internet.

Este sistema va a tener un asombroso impacto. Imaginemos un billón de personas conectadas físicamente, por medio de los bienes materiales, de la misma manera que las telecomunicaciones nos conectan a la información. Imaginemos la creación de la próxima gran red que conecte a las personas de manera material. En resumen, hablamos de un nuevo concepto de red de transporte que se basa en la idea de internet. Es descentralizada, es peer-to-peer, es bidireccional, versátil, con una baja inversión en infraestructura y que produce una mínima huella ecológica. Esperemos que el desarrollo de esta tecnología dé lugar un nuevo sistema de transporte. Uno que brinde nuevas opciones y que contribuya a crear un mundo en el que merezca la pena vivir.