

## **La cuestión de la privacidad de datos. Disposición 20/2015 del Ministerio de Justicia y Derechos Humanos sobre Protección de Datos Personales**

The data privacy issue. Provision 20/2015 of the Ministry of Justice and Human Rights on Personal Data Protection

Pablo A. Pirovano<sup>1</sup>

### *Resumen*

La tecnología robótica ha generado una revolución en la actividad de la aviación. Uno de los avances más importantes de este siglo XXI se ha dado a partir de la incursión masiva en el comercio privado de los Vehículos Aéreos No Tripulados (VANT o drones). Estos vehículos evolucionan día a día y en la actualidad son capaces de acceder a los sitios más recónditos pudiendo capturar información de forma tal que pueden pasar desapercibidos durante su tarea. La legislación advirtiendo la posibilidad de que la privacidad de las personas se vea seriamente afectada por la actividad de los VANT's, se encuentra forzada a regular su operatoria. En este capítulo analizaremos la normativa que la República Argentina ha diseñado para proteger los datos personales de las Personas Humanas que pueden verse afectadas por la acción de un VANT que transporte un dispositivo para capturar datos. Partiremos de la ley 25.326 como legislación general de protección de datos personales y repasaremos las disposiciones europeas sobre la materia que han servido de antecedentes para la regulación nacional.

### *Abstract*

The robotic technology has generated a revolution in the activity of aviation. One of the most important advances of the XXI century has been given from the massive incursion on the private market of the Remotely Piloted Aircraft Systems (RAPS or drones). These vehicles evolve day to day and at present they are capable of accessing to the most remote places being able of capturing information in such a way that they may go unnoticed during their task. The legislation noting the possibility that the privacy of the people is seriously affected by the activity of the RAPS's, is forced to regulate their operations. In this chapter we will analyze the regulations that the Argentine Republic has designed in order to protect the personal data of the Human Persons that may be affected by the action of a RAPS that carries a device so as to capture data. We will

---

<sup>1</sup> Abogado de la Universidad de Buenos Aires (1991). Programa Master ESEADE (1993). Socio de P&BA Pirovano & Bello, Abogados. Autor de numerosos artículos para las Editoriales La Ley y El Derecho y los portales de internet Abogados.com e Infobaeprofesional.com. Profesor invitado en el Premaster en Derecho Empresarial de la Universidad Austral y de los cursos de actualización en Derecho Empresarial de IDEA.

depart from the law 25.326 as general legislation of personal data protection and we will review the European provisions on the subject that have helped as background for the national regulation.

### *Palabras claves*

Vehículos Aéreos No Tripulados. Drones. Protección de Datos Personales. Imágenes audiovisuales. Intimidación. Privacidad. Derechos Civiles. Libertad. Ley 25.326. Disposición 20/2015.

### *Key words*

Remotely Piloted Aircraft Systems. Drones. Protection of Personal Data. Audiovisual Images. Intimacy. Privacy. Civil Rights. Freedom. Law 25.326. Regulation 20/2015.

## **Introducción**

La Disposición número 20/2015 de la Dirección Nacional de Protección de Datos Personales, que depende del Ministerio de Justicia y Derechos Humanos, reglamentó la captura y el tratamiento de datos personales mediante aeronaves pilotadas en forma remota, comúnmente denominadas drones, las que llevan la denominación de VANT conforme la Disposición.<sup>2</sup>

La norma establece que con las imágenes logradas por un VANT que incluyan información personal deben tomarse las mismas precauciones y recaudos que con cualquier base de datos de información personal. Pero, a la vez, libera de algunas obligaciones y da un tratamiento especial a quienes usen drones con fines recreativos.

La Disposición sustentada en la Ley 25.326 dispone que requieren reglamentación las fotografías y/o filmaciones y/o sonidos de personas que constituyendo una base de datos permitan realizar actividades de tratamiento de datos personales, en especial los que sean colectados a través de nuevos dispositivos y sistemas, que por sus particularidades y eventual peligrosidad pueden perjudicar los derechos de las personas.

---

<sup>2</sup> La denominación que refiere a Vehículos Aéreos No Tripulados. Enseña Carlos María Vasallo que los términos vigentes utilizados en las reglamentaciones jurídicas internacionales proyectadas como existentes son: Sistemas Aéreos no Tripulados (UAS) y Sistema de Aeronaves pilotadas en forma remota (RPAS). La Organización de Aviación Civil Internacional considera a los RPAS como un subconjunto de UAS. La distinción radica en la capacidad de un piloto remoto, para gestionar activamente el vuelo en tiempo real, al igual lo hace el piloto de una aeronave tripulada. Los sistemas de aviones no tripulados (UAS) tienen una variedad de formas y tamaños para servir a diversos propósitos generalmente de trabajo aéreo. Pueden tener una envergadura tan grande como un avión jet o menor que un modelo de avión de radio control.

De tal forma, el organismo regulador de las bases de datos personales ha entendido que la utilización de los VANT que posean bases de datos deben estar reglamentados y registrados los archivos que con ellos se conformen.

### **Protección de datos en el mundo**

La distribución geográfica de los países que cuentan con normas específicas de protección de datos y con autoridades encargadas de garantizar su aplicación es heterogénea. Es en Europa donde la protección de datos se encuentra alcanzando el nivel más importante en cuanto legislación sobre la materia. En casi la totalidad de los países europeos puede encontrarse estas disposiciones. Del mismo modo, América del Norte ha desarrollado un sistema legal de protección de datos, pero más centralizado a la privacidad individual, derecho que ha alcanzado un importante nivel de desarrollo. Siguiendo esta línea legislativa, en la última década tanto Latinoamérica como algunos países de África han producido avances importantes en cuanto a la institucionalización de esta protección.

### **Países con autoridad de protección de datos**

Habitualmente, la existencia de leyes que regulan los tratamientos de datos personales va acompañada del establecimiento de autoridades de supervisión encargadas del control del cumplimiento de esas leyes. En Europa, resulta trascendental que las autoridades de protección de datos personales sean independientes. No sucede lo mismo en otras áreas geográficas donde esa independencia se valora o pone en práctica de formas diferente a como sucede en Europa.

La Conferencia Internacional de Comisionados de Protección de Datos y Privacidad<sup>3</sup> exige que los países miembros cumplan una serie de requisitos, entre los que se incluyen la independencia en el ejercicio de sus funciones y la supervisión de normas específicas de protección de datos. En algunos países existen también autoridades subnacionales territoriales o sectoriales. Igualmente, un reducido número de países tienen normativa en la materia pero no han encomendado el control de su aplicación a autoridades específicas.<sup>4</sup>

### **Países con nivel adecuado de protección**

---

<sup>3</sup> Las Conferencias Internacionales comenzaron a celebrarse en Bonn en 1979. Su objetivo es el de reunir anualmente no sólo a las diferentes autoridades de supervisión de protección de datos y privacidad de todo el mundo, sino también a representantes del sector privado y a la sociedad civil. La organización corre a cargo de una autoridad anfitriona, que es designada, de entre las candidaturas presentadas, en la edición anterior. La Conferencia no es una organización internacional, sino un foro de encuentro, intercambio y discusión.

<sup>4</sup> En Latinoamérica únicamente Argentina y Uruguay poseen autoridades estatales que regulan la registración de las bases de datos personales.

El concepto de nivel adecuado de protección o "adecuación" está relacionado con la protección de datos en la Unión Europea. La Directiva 95/46<sup>5</sup> prohíbe la transferencia de datos a países que no cuenten con un nivel adecuado de protección de datos y establece un procedimiento para determinar formalmente si un país ofrece ese nivel de protección. En síntesis, la decisión corresponde a la Comisión, previa consulta al Grupo del Artículo 29<sup>6</sup> y a un Comité de representantes de los Estados miembros, que valora una serie de elementos como son la existencia de leyes de protección de datos, el contenido de esas leyes y el funcionamiento en la práctica del sistema de protección de datos. El Grupo de Autoridades del Artículo 29 adoptó un Dictamen en el que se desarrollaban los criterios de adecuación.

La principal consecuencia de que un país sea declarado adecuado es que se podrán transferir datos desde los Estados miembros de la Unión Europea sin necesidad de ningún tipo de trámite o autorización especial. La República Argentina se encuentra entre los países considerados adecuados.

### **La ley 25.326. Reglamentación del Artículo 43 de la Constitución Nacional**

El sustento supralegal de la ley 25326 se encuentra en la garantía de Hábeas Data que fuera incorporada por la reforma constitucional de 1994 en el tercer párrafo del artículo 43 de la Constitución Nacional, en estos términos:

*"...Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, la rectificación, confidencialidad o actualización de aquellos. No podrá afectarse el secreto de las fuentes de información periodística".*

Esta incorporación efectuada a nuestra norma fundamental tiene basamento en el derecho a la privacidad e intimidad reconocido como garantía constitucional en el artículo en el artículo 19 de la Constitución Nacional. Este protege jurídicamente en relación directa con la libertad individual, un ámbito de autonomía personal, así como acciones, hechos y datos que, conforme a las formas de vida acogidas por la sociedad,

---

<sup>5</sup> Se trata de una Directiva sobre protección de datos de la Unión Europea.

<sup>6</sup> El Grupo de Trabajo del Artículo 29 (GT 29), creado por la Directiva 95/46/CE, es un órgano consultivo independiente integrado por las Autoridades de Protección de Datos de todos los Estados miembros, el Supervisor Europeo de Protección de Datos y la Comisión Europea. Las funciones del GT29 reconocidas por la Directiva incluyen estudiar toda cuestión relativa a la aplicación de las disposiciones nacionales tomadas para la aplicación de la Directiva, emitir dictámenes sobre el nivel de protección existente dentro de la Comunidad y en países terceros, asesorar a la Comisión sobre cualquier proyecto de modificación de la Directiva, y formular recomendaciones sobre cualquier asunto relacionado con la protección de datos en la Unión Europea.

están reservadas al individuo, y cuyo conocimiento y divulgación por extraños implica peligro real o potencial para la misma intimidad.<sup>7</sup>

Del mismo modo, en el ámbito supranacional una primera aproximación de protección en la esfera íntima de la persona se encuentra enunciada dentro de la Declaración Universal de los Derechos Humanos de 1948, cuyo artículo 12 señala: “*Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o su reputación. Todo persona tiene derecho a la protección de la ley contra tales injerencias o ataques.*”

El derecho a la intimidad abarca aquello que se considera más propio y oculto del ser humano —entendiéndose por propio y oculto la información que mantiene para sí mismo—. Pero es insoslayable que el contacto permanente del ser humano con sus semejantes al interior de la sociedad a la que pertenece, así como todos aquellos avances tecnológicos que han venido desarrollándose en la sociedad, han comenzado a transgredir aquellos ámbitos que forman parte de la intimidad del ser humano.<sup>8</sup>

Un derecho tal como ha sido reconocido por las normas puede justificarse por su capacidad de promover ciertos bienes básicos para los ciudadanos: como es la libertad, la igualdad, la seguridad y otros semejantes. Por lo que desde esta perspectiva puede justificarse la intimidad como un medio para promover la libertad individual,<sup>9</sup> lo que Constant denominó “*el goce pacífico y la independencia privada*”,<sup>10</sup> mientras Stuart Mill estableció que “*la única libertad que merece este nombre es la de buscar nuestro propio bien a nuestra propia manera*”.<sup>11</sup> Por lo que la protección de este derecho frente a cualquier intromisión injustificada del gobierno en la esfera privada del individuo, fueren cuales fueren los medios empleados, debía ser considerada una exigencia de la cuarta enmienda de la Constitución americana, por tanto, garantizó a los ciudadanos la seguridad de su persona, de su domicilio y de sus efectos frente a cualquier intromisión indebida.<sup>12</sup>

En la actualidad y como consecuencia de los avances tecnológicos, la intimidad en lo jurídico ha dejado de tener un sentido únicamente individual. De forma paulatina

---

<sup>7</sup> CSJN, 11-12-84, E. D. 112-239.

<sup>8</sup> GARCÍA GONZÁLEZ, Aristeo. *La Protección de Datos Personales: Derecho Fundamental del Siglo XXI. Un Estudio Comparado*. Boletín Mexicano de Derecho Comparado, nueva serie, año XL, núm. 120, septiembre-diciembre de 2007, pp. 743-778.

<sup>9</sup> GARCÍA SAN MIGUEL, Luis, *Estudios sobre el derecho a la intimidad*, Madrid, Tecnos, p. 17 y ss.

<sup>10</sup> Cfr. CONSTANT, Benjamín, *Sobre el espíritu de conquista*, Madrid, Pág. 75. De su conferencia en el ateneo de París en 1891, publicada con el título “De la libertad de los antiguos comparada a la de los modernos”, en donde señalaba que mientras los antiguos gozaban del derecho a intervenir en los asuntos públicos, pero carecían de libertades en el orden individual, los modernos sin renunciar a la libertades políticas señalaban que la libertad debía componerse del goce pacífico y de la independencia privada.

<sup>11</sup> STUART MILL, John, *Sobre la libertad*, 6a. reimp., Madrid, Alianza Editorial, pp. 126-152.

<sup>12</sup> WARREN, Samuel y BRANDREIS, Louis, *El derecho a la intimidad*, Madrid, Civitas, p. 19 y ss.

se ha posicionado como una necesidad pública y colectiva, ello en pos de resguardar y controlar la información relevante a los individuos que es utilizada por los distintos agentes sociales. En tal sentido se ha dicho que cada ciudadano fichado en un banco de datos se halla expuesto a una vigilancia continua e inadvertida que afecta potencialmente incluso a los aspectos más sensibles de su vida privada. Aquellas personas que en épocas anteriores dejaban que sus datos personales estuvieran fuera de todo control, por su variedad y multiplicidad, hoy, además de tomar conciencia de ello, comienzan a exigir un reconocimiento sobre su uso y control.<sup>13</sup>

Así es que luego de extenderse los confines del derecho a la intimidad a toda información personal, se pasó a identificar un bien jurídico autónomo —denominado intimidad informativa, libertad informática o autodeterminación informativa— sólo en parte coincidente con aquélla, al menos en la noción que de la misma o de la vida privada ha prevalecido en los distintos ordenamientos. Este bien jurídico consiste en asegurar a las personas el control de la información —de los datos— que les es propia para ponerles al resguardo o, al menos, permitirles protegerse de los perjuicios derivados del uso por terceros, públicos o privados, de ese material. Las ilimitadas posibilidades que ofrece la tecnología de captar, acopiar, asociar, recuperar en tiempo real y conservar indefinidamente datos personales, así como de obtener ulterior información personal mediante su tratamiento, junto a la necesidad creciente de los mismos en todo tipo de relaciones, han hecho imprescindible garantizar a los individuos instrumentos jurídicos que hagan posible ese control.<sup>14</sup>

En nuestro país el legislador ha interpretado el alcance del artículo 43 párrafo tercero de la Constitución Nacional, estableciendo una serie de reglas y principios para los archivos públicos y privados destinados a dar información. A partir de esa necesidad social, la ley 25.326 tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre.

El objeto de la ley no es otro que garantizar el honor y la intimidad de las personas,<sup>15</sup> y tiene alcance a todas aquellas circunstancias mediante las cuales el complejo de derechos personalísimos, que incluyen la privacidad y la identidad, relacionados a su vez con la imagen y con los conceptos de verdad e igualdad se encuentren involucrados. Lo que se pretende lograr es la autodeterminación informativa que consiste en el desarrollo que toda persona tiene a controlar la información que le

---

<sup>13</sup> FROSINI, Vittorio, *Cibernética, derecho y sociedad*, Madrid, Tecnos, pp. 178 y 179. Este autor afirma que la vida individual y social corre el riesgo de hallarse sometida a un “juicio universal permanente”.

<sup>14</sup> MURILLO DE LA CUEVA, Pablo Lucas y PIÑAR MAÑAS, José Luis. *El derecho a la autodeterminación informativa*. Fundación Coloquio Jurídico Europeo. Madrid. 2009. pp. 17 y ss.

<sup>15</sup> PIROVANO Pablo. A.. *Las facultades de contralor y sanción derivadas de la Ley de Protección de Datos Personales*. Revista Legislación Argentina. Editorial El Derecho. 8/10/2010.

concierno, sea íntimo o no, para preservar de este modo y en último extremo, la propia identidad, su dignidad y libertad. El bien jurídico tutelado es el derecho a la veracidad de la información<sup>16</sup>.

En el sentido antes apuntado, el derecho a la intimidad ya no se reduce a excluir a los terceros de la zona de reserva, sino que se traduce en la facultad del sujeto de controlar la información personal que de él figura en los registros, archivos y bancos de datos, sean estos públicos o privados.

La ley 25.326 reglamenta el tratamiento de los datos personales y tiene por objeto: *"la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional"*.

Interpretando al constituyente, el legislador ha instaurado un sistema de registro público de todos aquellos archivos, registros o banco de datos que no sean para un uso exclusivamente personal, sin distinguir entre aquellos que estén destinados a proveer informes o no.<sup>17</sup> De tal modo que se encuentran excluidos de las normas de protección, los registros o archivos de uso personal o doméstico siempre y cuando no excedan el uso personal de quien los administra.

### **Datos destinados a dar informes**

Debe entenderse por banco de datos destinado a proveer informes a aquel registro, archivo, base o banco de datos que permita obtener información sobre las personas, se transmitan o no a terceros; dado que el tratamiento implica un riesgo susceptible de causar un perjuicio al titular del dato. Asimismo, al ser el derecho a controlar la información personal un derecho humano, debe interpretarse a favor de las personas.

La Real Academia Española define a la palabra "informe" como: *"Descripción oral o escrita de las características o circunstancias de un suceso o asunto"*. Entonces "banco de datos destinado a dar informes" equivale a "banco de datos destinado a describir algo sobre las personas".

De esta manera, conforme lo entiende la Dirección Nacional de Protección de Datos Personales cuando se accede a una base que interrelaciona datos y produce una

---

<sup>16</sup> COLAUTTI Carlos E. Revista La Ley 1996-C p. 917

<sup>17</sup>Conf. Art. 21 y 24 de la ley 25326.

serie de informaciones acerca de una persona determinada, se configura la acción requerida por la norma: "brindar informe".

En ninguna parte de la norma se indica que, para que la protección de la ley adquiera virtualidad, debe tratarse de un destino único y exclusivo a brindar informes. Para que rija la protección de la ley alcanza con que uno de los usos que se le da a la base de datos sea brindar información o describir algo sobre una persona determinada o determinable.

Tampoco la norma exige que el destinatario del informe deba ser una tercera persona ajena al responsable o usuario de la base de datos, sino que también abarca los usos internos de la información personal.

Al tiempo del dictado de la ley existían dudas respecto del significado que debía dársele a la expresión "privados destinados a proveer informes" y a la posibilidad de que a partir de su vaguedad, una gran cantidad de archivos, registros o bases de datos pudieran quedar excluidos del régimen creado, o al menos de una buena parte de sus disposiciones<sup>18</sup>.

El Poder Ejecutivo intentando poner fin a cualquier incertidumbre generada por la ley, estableció en el Art. 1° del decreto 1558/2001 que *quedan comprendidos en el concepto de archivos, registros, bases o bancos de datos privados destinados a dar informes, aquellos que exceden el uso exclusivamente personal y los que tienen como finalidad la cesión o transferencia de datos personales, independientemente de que la circulación del informe o la información producida sea a título oneroso o gratuito.*

Por tanto, aquellos archivos, registros o bancos de datos privados que no tienen como finalidad principal suministrar informes a terceros, pero que recolectan información personal pasible de ser utilizada, deben también ser objeto de inscripción. El objetivo de la norma es resguardar incluso aquellos datos personales registrados en un archivo, registro o banco de datos que no está destinado a dar informes.

De tal forma, registros tales como los de personal, bancarios, agencias de empleos y de compañías de seguros, entre otros, se encuentran incluidos en la cláusula constitucional.<sup>19</sup> Por su parte Colautti<sup>20</sup> define que, "*... si en un banco o registro de datos existe información es para ser utilizada, aunque la finalidad específica del registro no sea proveer informes. El tema esta vinculado directamente con el derecho a una información verídica. .... es incontrovertible que la finalidad de todo registro de datos*

---

<sup>18</sup> TANUS Gustavo Daniel. *Protección de Datos Personales*, El Derecho 190-670

<sup>19</sup> EKMEKDJIAN Miguel Angel. *El Habeas Data en la reforma constitucional*. La Ley 1995-E, p. 946

<sup>20</sup> COLAUTTI Carlos E. *Reflexiones preliminares sobre el habeas data*. La Ley 1996-C, p. 917

*consiste en ser utilizado. La única diferencia puede consistir en el ámbito temporal,..... Es de prever que los datos algún día serán utilizados y conocidos por terceros.*"<sup>21</sup>

### **Uso Exclusivo Personal**

Como se señalara, se obliga a inscribir en el Registro las bases de datos que no sean para uso exclusivo personal (art. 24 de la ley 25.326). El concepto de "uso exclusivo personal" se interpreta unánimemente de la manera más favorable al ejercicio del derecho a controlar la información personal.

Por ello, corresponde interpretar este concepto "como uso exclusivo de la persona titular del banco de datos", entendida como aquella que, por conservarse en la esfera íntima de la persona, no trasciende a terceros y/o no tiene razonable potencialidad de dañar un derecho del titular del dato (ejemplo: archivo de direcciones de amistades).

Debe colegirse entonces que el instituto reglamentado por la Ley 25.326 protege la intimidad de las personas en relación a los datos personales depositados en archivos, registros o bancos de datos soportados por cualquier medio, ello en la medida que no sean para uso exclusivamente personal.

### **La Reglamentación del debido contralor de los registros, archivos y bases de datos. Facultades sancionatorias**

Como fue analizado, el legislador quiso proteger derechos relacionados con la intimidad de las personas, pero asociados al tráfico mediante cesión de datos personales, siempre partiendo de *archivos, registros, bases o bancos de datos privados destinados a dar informes, o que excedan el uso exclusivamente personal.*

Dentro del marco reglamentario del Art. 31 de la ley 25.326 fue dictado el Decreto 1160/2010. Mediante esta normativa el Poder Ejecutivo estableció un régimen de contralor de los archivos, registros y bases de datos. Se ha motivado el mismo en *"la necesidad de establecer un procedimiento que regule con mayores precisiones y simplifique la actividad de la Dirección Nacional de Protección de Datos Personales relativa a sus funciones de investigación y control, con miras a la procedencia de la aplicación de sanciones, con resguardo de las reglas del debido proceso y del derecho de defensa."* La autoridad de contralor entre otras prerrogativas podrá iniciar los

---

<sup>21</sup> En igual sentido ver "Evans, Nélsón E. s/Acción de Habeas Data". S CAN1 TW 000C 000015 21-06-01 Magistrado: Vergara. Morello, Sosa y Berizonce, "Códigos Procesales.", t. V-A, pp. 143 y 148, Librería Editora Platense -Abeledo-Perrot, 1991; De Santo, "La prueba judicial", p. 92, Editorial Universidad, 1992 Alterini, Ameal, López Cabana, "Derecho de Obligaciones civiles y comerciales", p. 123 y s., Abeledo-Perrot, 4a. ed., 1993; CANE, Sala "B", c. 16.814, S.D.C. 10/2001 Rezzónico, "Estudio de las Obligaciones", t. I, pp. 776/777 Arazi y Rojas, "Código Procesal.", t. I, pp. 257/258, Rubinzal-Culzoni Editores, 2001.

procedimientos de oficio o por denuncia de quien invocare un interés particular, ello de la misma forma que lo preveía su redacción original.

Adicionalmente detalla las acciones que podrá desarrollar el organismo de contralor para el cumplimiento de sus cometidos, con un nivel de injerencia sobre el objeto de control que permite avizorar –teniendo presente la motivación sancionatoria– una ingente actividad administrativa que por su parte deberá ser contrapesada por un férreo control judicial.

En tal sentido es importante precisar qué ejercicio del poder de policía en el ámbito del honor y la intimidad de las personas, en multiplicidad de ocasiones se habrá de contraponer al derecho de propiedad del *hardware* y *software* de quien administra esos archivos, registros o bases de datos. Es evidente que de darse ello, deberá el Poder Judicial efectuar el control suficiente y exhaustivo de lo actuado por la autoridad de contralor, cuando así sea requerido por el administrado, siendo fundamental que se efectúe una prudente utilización de la facultad reglamentaria conferida por el Poder Ejecutivo, ya que ella solamente apunta a los sistemas que son utilizados en archivos, registros o bases de datos para tratar los mismos.

Operar el control de modo tal que avance sobre el contenido de los registros o archivos, implicaría poner en riesgo otras garantías republicanas –en este caso de los responsables de los registros, archivos o bases de datos e incluso de los propios titulares de los datos– suponiendo ello una injerencia del Estado no deseada por la norma bajo análisis.<sup>22</sup>

### **Las regulaciones europeas sobre cesión de Datos Personales a través de VANT's**

Conforme surge del dictamen de la Comisión Europea al Parlamento Europeo del 8 de abril de 2014<sup>23</sup> las operaciones de los VANT's no deberán ser de naturaleza tal que infrinjan los derechos fundamentales, incluidos el derecho a la intimidad personal y familiar y la protección de los datos personales. Dentro de la amplia gama de aplicaciones civiles potenciales de los VANT's, los hay que pueden implicar la recogida de datos personales y suscitar problemas de orden ético, de protección de la intimidad o de datos personales, en particular en los ámbitos de la vigilancia, el seguimiento, la cartografía o los registros de vídeo. Los operadores de VANT's tendrán que cumplir las disposiciones aplicables en materia de protección de datos, en particular las indicadas

---

<sup>22</sup> PIROVANO Pablo A. *Las facultades de contralor en el régimen de protección de datos personales.* Revista legislación Argentina. 8 de Oct. de 2010. Editorial El Derecho.

<sup>23</sup> Comunicación de la Comisión al Parlamento Europeo y al Consejo. *Una nueva era de la aviación. Abrir el mercado de la aviación al uso civil de sistemas de aeronaves pilotadas de forma remota de manera segura y sostenible.* Bruselas, 8 de Abr. de 2014.

en las medidas nacionales establecidas de conformidad con la Directiva 95/46/CE<sup>24</sup> sobre la protección de los datos personales y la Decisión Marco 2008/977.<sup>25</sup> Los riesgos identificados con mayor frecuencia están relacionados con el uso de equipos de vigilancia instalados en VANT's. El tratamiento de datos personales deberá realizarse siempre por razones legítimas. Por consiguiente, la apertura del mercado de la aviación a los VANT's debe implicar una evaluación de las medidas necesarias para garantizar el respeto de los derechos fundamentales y la protección de los datos personales, así como de la intimidad. El aspecto de la protección de la intimidad exigirá un seguimiento continuo por parte de las autoridades competentes, incluidas las autoridades nacionales de supervisión de la protección de los datos personales.

De acuerdo al Dictamen 01/2015 del Grupo de Trabajo del artículo 29 (GT29) es necesario centrarse en el desafío que un número ilimitado de VANT's podría provocar a la privacidad de las personas y las libertades civiles y políticas a la vez que deben ser evaluadas las políticas necesarias para garantizar el respeto de los derechos fundamentales y la protección de datos. Dando cuenta de la dificultad antes apuntada indica el Dictamen que la falta de transparencia de la operación de los VANT's por la dificultad de detección visual desde el suelo así como la dificultad para precisar el equipo de tratamiento de datos portan como sus fines específicos, denotan riesgos concretos para la privacidad de las personas. Uno de los riesgos para los derechos y libertades de las personas que refiere el Dictamen es el derivado de la utilización de drones para fines policiales.

El Dictamen indica que es aconsejable: i) una autorización específica de las Autoridades de Aviación Civil (AAC) cuando la legislación nacional permita operar un VANT; ii) la búsqueda de los criterios más adecuados para el tratamiento legítimo, cumpliendo con el principio de limitación de finalidad, el principio de minimización de los datos y el principio de proporcionalidad (mediante la elección de la tecnología más apropiada junto a las medidas para evitar la recogida de datos personales innecesarios) del modo más equilibrado para el caso que nos ocupa; iii) El principio de transparencia (informando a los interesados de los tratamientos llevados a cabo) son obligaciones que deben cumplirse antes de operar un VANT.

Aborda recomendaciones a los gobiernos europeos para el fortalecimiento de un marco que garantice el respeto de los derechos fundamentales en juego, tanto el de la protección de datos personales introduciendo la idea del uso responsable de los VANT's. Se solicita a los responsables políticos la introducción de los principios de protección de datos entre las principales características de las disposiciones nacionales

---

<sup>24</sup> Directiva 95/96CE relativa a la protección de las personas físicas en relación a los datos personales y la libre circulación de esos datos DO L 281 del 23 de Nov. de 1995. pp. 31-50.

<sup>25</sup> Decisión Marco 2008/977 del Consejo del 27 de Nov. de 2008 relativa a la protección de datos personales tratados en el marco de la cooperación judicial y policial en materia penal.

que regulen el uso comercial de los VANT's. Por último, se recomienda una estrecha colaboración con las Agencias de Protección de Datos Personales.

En este marco, se ha prestado atención la responsabilidad en los tratamientos de datos, especialmente teniendo en cuenta la amplia gama de servicios basados en VANT's, que ya son ofrecidos por empresas especializadas para organizaciones públicas y privadas. A la luz de esto, es de la mayor importancia que el Responsable del tratamiento y el Encargado del tratamiento deben estar claramente identificados para cada tipo de operación llevada a cabo por drones, mediante la consideración de los elementos clave para distinguir al Responsable del tratamiento de otros actores. Una guía clara para identificar las diferentes combinaciones de responsabilidades entre las diferentes entidades que participan en la tramitación conjunta se puede encontrar en el Dictamen 1/2010 del GT29 en los conceptos de "Responsable del tratamiento" y "Encargado del tratamiento".

De acuerdo a la Directiva existen exenciones y excepciones a las directrices que están dadas en el marco de las operaciones civiles. En tal sentido, las operaciones con datos personales que se encuentren dentro del ámbito personal y exclusivo de la persona que los administre no está dentro del alcance de la Directiva.

Asimismo, la Directiva de protección de datos prevé que los Estados miembros tendrá la posibilidad de disponer exenciones o excepciones a algunas de sus disposiciones en caso de tratamiento de datos personales llevados a cabo exclusivamente con fines periodísticos o con el propósito de expresiones artísticas o literarias. No obstante, solo deben ser las necesarias para conciliar el derecho a la intimidad con las normas que rigen la libertad de expresión. Entonces, mediante el uso de VANT's tampoco podrán avanzarse sobre la intimidad de las personas aún en el marco de una investigación periodística.

El tratamiento de datos personales captados mediante VANT's en el ámbito de la Comisión Europea debe respetar el Artículo 7 de la Directiva. El Dictamen en ese orden recuerda que debe existir interés legítimo, el que sirve de orientación en este punto. Por ello, deberá ser tenido en cuenta de acuerdo a los propósitos del tratamiento en juego: i) el consentimiento libre, específico e informado; ii) que se efectuó en el marco de un contrato en el que el interesado sea parte; iii) que sea necesario para el cumplimiento de una obligación legal; iv) que se en ocasión de proteger el interés vital del interesado, y; v) cuando se trata de la ejecución de una actividad en interés legítimo del responsable del tratamiento.

Como consecuencia, la potencial afectación a la intimidad y las libertades civiles que podría deparar la apertura del mercado de la aviación para VANT's el GT29 ha llamado la atención de los legisladores europeos, fabricantes de VANT's y de los equipos y operadores, mediante recomendaciones destinadas a proporcionar una guía

adicional a las diferentes opiniones y dictámenes referidos al tratamiento específico de datos.

Las directivas apuntan tanto a nivel europeo como nacional a establecer un marco para garantizar no sólo la seguridad de vuelo, sino también el respeto de todos los derechos fundamentales. En esta perspectiva, el GT29 exige un compromiso de las partes interesadas en el debate relativo a la integración de los drones en el espacio aéreo civil. Para ello las partes implicadas deben consensuar:

- La armonización y la modernización de las políticas pertinentes de los Estados miembros en relación con VANT's, incluyendo cuestiones respecto a la ley aplicable a las operaciones con VANT's que se efectúen en dos o varios países;
- La introducción, como parte del marco anterior, de las normas específicas que garanticen un uso responsable de los VANT's, que debe incluir necesariamente el respeto a las áreas privadas (tales como jardines, patios, terrazas, etc.); a tal fin, puede preverse la introducción, cuando sea necesario, de los perímetros virtuales - o zonas de exclusión aérea -. Además, dado que el uso de VANT's pueden limitarse a áreas muy específicas en muchos Estados miembros, la publicación de mapas ayudaría a los usuarios a entender donde se permite el uso de VANT's;
- La introducción de una obligación, a nivel europeo y/o nacional, para que los fabricantes de pequeños VANT's para el mercado único los embalen junto a información suficiente (por ejemplo dentro de las instrucciones de servicio) en relación con la intrusión potencial de estas tecnologías y recordando la necesidad de respetar la legislación y los reglamentos que protegen la privacidad, la protección de datos personales y otros derechos fundamentales.
- El desarrollo y la introducción por parte de los responsables políticos competentes, a nivel europeo y/o nacional, en estrecha consulta con los representantes de la industria, de criterios de evaluación de impacto en la protección de datos que la industria y los operadores pueden utilizar fácilmente;
- La introducción de los aspectos de protección de datos entre las principales características de las disposiciones nacionales que regulan el uso comercial de VANT's (en relación con la competencia del piloto y la formación, entre los requisitos de aeronavegabilidad y certificación, además de la emisión/revocación de licencias de explotación y permisos de trabajo aéreas, etc.); en particular, las declaraciones de haber tenidos en cuenta los requisitos de protección de datos podrían ser parte de las condiciones en que se concederá un permiso;
- La promoción de certificaciones de protección de datos con el fin de mejorar la concientización y la comprensión de las cuestiones de protección de datos de los operadores de drones civiles, así como con el fin de supervisar su cumplimiento;
- Además, el GT29 recomienda que la Comisión Europea haga uso de programas de financiación para apoyar las investigaciones e inversiones para nuevas tecnologías destinadas a aumentar la transparencia (nuevas tecnologías para informar al público en general de la existencia de drones voladores, y sus fines, y poder así ejercer sus derechos de acceso), incluyendo, por ejemplo, placas de matrícula inteligentes o

disponer de un sitio web que publique la información en tiempo real acerca de todas las operaciones mediante drones.

### **La Disposición 20/2015. Las facultades conferidas por la ley 23.526**

El Estado Argentino dispuso la regulación del tratamiento de datos captados por medio de VANT's, por intermedio de la Disposición 20/2015 que reglamenta el uso de las fotografías y/o filmaciones y/o sonidos de personas que, constituyendo una base de datos, permitan realizar actividades de tratamiento de datos personales, en cuanto sean colectados a través de nuevos dispositivos y sistemas de aviación no tripulada (VANT), que por sus particularidades y eventual peligrosidad pueden perjudicar los derechos de las personas.

La reglamentación se ha dictado aduciendo el uso de las facultades conferidas en el artículo 29, inciso 1, apartado b) de la Ley N° 25.326 y el artículo 29, inciso 5, apartado a) del Anexo I del Decreto N° 1558/01.

A partir de lo apuntado y lo que venimos estudiando, no resulta ser objeto de la ley 25326 la reglamentación del uso del espacio aéreo y a otras cuestiones relacionadas con la operación específica de los VANT's, aun cuando se pretenda reglamentar el uso de los archivos que son conformados a partir del uso de un VANT.

La Disposición colecta muchas de las recomendaciones del Dictamen 01/2015 de la Comisión Europea, y centra su objetivo en el adecuado uso de los VANT's y en la registración de las bases de datos, sin adentrarse en otros aspectos tratados en la Disposición 01/2015.

La Disposición refiere al Art. 2 de la ley 25.326 que define a las bases de datos "como el conjunto organizado de datos personales<sup>26</sup> que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso". A continuación se señala que los datos personales contenidos en fotografías y videos deben recibir el trato de una base de datos y por lo tanto están sujetos al régimen de la ley de protección de datos personales "en tanto se refiere a una persona determinada o determinable". El regulador considera que "una imagen o registro fílmico o sonoro de las personas

---

<sup>26</sup>Definición de "Dato" según REAL ACADEMIA ESPAÑOLA. Recuperado el 18 de nov. de 2015.  
<http://dle.rae.es/?w=diccionario>

1. m. Información sobre algo concreto que permite su conocimiento exacto o sirve para deducir las consecuencias derivadas de un hecho.
2. m. Documento, testimonio, fundamento.
3. m. Inform. Información dispuesta de manera adecuada para su tratamiento por una computadora.

constituye, a los efectos de la Ley N° 25.326, un dato de carácter personal”, por lo que su tratamiento constituye una base de datos sujeta al régimen de la ley.

Por último, se considera a los VANTs´ como medios de recolección de datos fotográficos, fílmicos y sonoros de personas que generan un importante riesgo para los derechos a la privacidad y a la autodeterminación informativa. Diferencia al VANT de una cámara de video vigilancia porque esta se encuentra en una posición fija y aquellos pueden desplazarse, por lo que los define como dispositivos que encierran una afectación particular a la privacidad.

Entonces a partir de esta reglamentación resultan alcanzadas por la Ley 25.326 aquellas actividades de recolección de datos personales que contengan material fotográfico, fílmico, sonoro o de cualquier otra naturaleza, en formato digital, que sean realizadas mediante VANT´s, y que tengan por objeto su almacenamiento en dispositivos o cualquier otro tratamiento posterior.

La Disposición 20/2015 en línea con la normativa que reglamenta, prevé en relación a los VANT`s que su uso no debe afectar el derecho a la intimidad de las personas. Y quienes registren imágenes de terceros deberán, en el tratamiento de esos datos, cumplir con lo dispuesto por la ley 25.326. Por ejemplo, deberán dar acceso a esos datos a sus titulares.

En este mismo sentido, la nueva norma determina que los responsables de la recolección de datos personales a través de VANT´s “deberán contar con un manual o política de tratamiento de datos personales y privacidad” e inscribir en el Registro Nacional de Bases de Datos todas aquellas bases de datos en las que se almacenen datos personales recabados mediante VANT´s. Este requisito es una novedad en el ámbito de la registración de bases de datos y solamente se solicita a los titulares de base de datos conformadas por VANT´s. Deberá ser objeto de interpretación que habrá de resolver el organismo de contralor en el caso que los datos se encuentren guardados en una base que ha captado imágenes con un VANT y también con otros instrumentos de filmación. Del mismo modo, abrigamos que la DNPDP no convierta al manual –mediante la exigencia de requisitos exagerados o de difícil cumplimiento- en un impedimento para la utilización lícita de los VANT´s.

### **Obligatoriedad de registración de las bases de datos y archivos captados a través de VANT´S**

El artículo 3 del Anexo I de la Disposición prevé que es obligatoria la registración de todas aquellas bases de datos de contenido audiovisual que se encuentran colectadas en ámbitos que excedan al privado de quien las ha producido y hayan sido

obtenidas mediante el uso de un VANT.<sup>27</sup> De esta forma, salvo algunas excepciones, como consecuencia de haber sido tomados con la ayuda de este medio de navegación aérea, los datos colectados por cámaras fotográficas y las videofilmadoras pasan a ser archivos sujetos a registración y los datos allí contenidos obligatoriamente deberán tener consentimiento del dueño de la imagen para poder ser lícitos.

Frente a esta reglamentación, cabe interrogarse, más allá de la comprensible capacidad de vuelo, cuál es el motivo para reglamentar de modo especial una base de datos o archivos audiovisuales captados con otros medios de aquellos captados con el auxilio de un VANT. Ello en virtud de que lo que la ley 25.326 regula es la existencia de bases de datos y archivos con destino a dar informes, sin importar quién o cómo se captan y dónde se graban, todo lo cual incluye la cesión y transferencia de datos (artículos 1 y 21), y el uso que exceda al exclusivamente personal de la base de datos (artículo 24). Entonces todo tipo de archivo audiovisual que cumpla esta condición debe ser registrado.

Por su parte, de entenderse necesario registrar todas las bases de datos constituidas por material audiovisual que no sean para uso exclusivamente personal y probado, llevaría en la práctica a la necesidad de registrar todos los archivos de la totalidad de las personas que poseen cámaras fotográficas y filmicas en la medida que sean utilizadas fuera del ámbito exclusivamente privado. Ello, como consecuencia del ámbito de control del Estado, quien únicamente está facultado a establecer la necesidad de registración de las bases de datos y archivos que conteniendo datos de terceros que no sean para uso privado de quien los detente. Entonces, un archivo guardado en una cámara fotográfica o videofilmadora, sea que se encuentre transportada en un VANT; en un avión controlado a distancia; en un vehículo terrestre o por una persona humana, deberá ser registrado si no es de uso exclusivo de la persona que lo ha obtenido. De ser así, una primera conclusión es que la Disposición 20/2015 reglamenta lo que ya estaba reglamentado.

La Disposición 20/2015 interpretando que la visión aérea que otorgan los VANT's y su capacidad de no ser detectables en algunos casos, podrían implicar un "importante riesgo" para los derechos a la privacidad y a la autodeterminación informativa, obliga a la registración de las bases de datos que se conformen a través de su utilización. Aun así será un desafío determinar cuándo es necesaria la registración, ya que la actividad fotográfica de un VANT puede o no constituir una "base de datos",

---

<sup>27</sup> Artículo 3: Deberán inscribirse en el REGISTRO NACIONAL DE BASES DE DATOS dependiente de esta DIRECCIÓN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES, todas aquellas bases de datos en las que se almacenen datos personales recabados mediante los VANTs o drones en los términos previstos por las Disposiciones DNPDP Nros. 2 del 14 de febrero de 2005, 3 del 4 de abril de 2005 y 10 del 18 de setiembre de 2006. Asimismo, al inscribirse, deberán denunciar, respecto de los VANTs o drones, sus finalidades y capacidades técnicas de los dispositivos de recolección de datos personales y adjuntar el manual de tratamiento de datos personales previsto en el artículo precedente."

que es la premisa que el legislador ha dispuesto para establecer la necesidad de registración. Es que no todo archivo constituye una base de datos. Por ello, la propia Disposición, siguiendo a la Ley 25.326 y al Decreto 1.558/2001 dispone que deberán ser registradas los archivos, registros, bases o bancos de datos privados destinados a dar informes, aquellos que exceden el uso exclusivamente personal y los que tienen como finalidad la cesión o transferencia de datos personales, independientemente de que la circulación del informe o la información producida sea a título oneroso o gratuito.

### **Consentimiento previo**

La Disposición 20/2015 no se detiene en la necesidad de registración de las bases de datos o archivos que contengan información de terceros que no sea de uso exclusivo y privado de su titular. También dispone las condiciones que debe cumplir la captura de imágenes mediante VANT's. La Disposición establece que deberá realizarse con el consentimiento de la persona filmada, remitiendo a lo previsto en los artículos 5 y 6 de la ley 25.326. En tal sentido, el Artículo 5 indica que el tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias. El referido consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y destacada, previa notificación al propietario de los datos de la información descripta en el Artículo 6 de la ley.

De la remisión a estos artículos de la ley 25.326 surge que quienes operen VANT's con cámaras filmadoras o fotográficas o algún otro medio de captura de imágenes o audio deberán tener el consentimiento de todas las personas que durante el vuelo puedan ser captadas, o bien abstenerse de realizar grabaciones. De tal modo, la actividad de los VANT's con medios de captura de imágenes o audio se verá muy limitada.

Asimismo, en cuanto a la posible actividad de los VANT's, la Disposición 20/2015 prevé que no será necesario el consentimiento cuando los datos se obtengan de: i) fuentes de acceso público irrestricto; ii) se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal; iii) deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento. Estas excepciones relacionadas con el consentimiento de las personas que pueden verse filmadas, fotografiadas o grabadas dejan establecido que siendo un archivo audiovisual obtenido en la vía pública o bien en aquellos casos en las imágenes o el audio son captadas dentro del ejercicio legal de la actividad estatal; o bien si son imágenes capturadas en el marco de una relación contractual o científica, se relacionan con cuestiones ineludibles en cuanto a que: a) lo que sucede en el ámbito público no puede jamás violar la intimidad de las personas y quienes se hayan expuesto de una determinada forma en el marco de un ámbito irrestrictamente público no están en posición de ejercer un derecho propio sobre quien haya captado imágenes de ellos; b) las imágenes relacionadas con la actividad lícita del Estado en tanto forme parte del ejercicio del poder de policía de modo alguno pueden

ser objetadas por aquellas personas que hayan sido captadas. Por supuesto que si se tratase de datos audiovisuales capturados fuera del marco conferido por la actividad lícita estatal, esta conducta estaría fuera del marco legal impuesto por la Ley 25.326 y la Disposición 20/2015.

La Disposición 20/2015 también remite al Artículo 6 de la ley 25.326. Esta norma legal prevé que cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara: a) la finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios; b) la existencia del archivo, registro, banco de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable; c) el carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos referidos en el artículo siguiente; d) las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos; e) la posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos.

Sin embargo, el consentimiento antes descripto no será necesario cuando los datos se recolecten en el marco de un acto público o "hecho sobre el que pueda presumirse la existencia de un interés general para su conocimiento y difusión al público".

Surge entonces de la norma en la que se basa la Disposición 20/2015 que debe existir el consentimiento de las personas cuyos datos son colectados a través de los VANT. Es previsible que este consentimiento sea de difícil implementación porque todo vuelo de un VANT distinto al que se pueda llevar a cabo en un acto público o respecto a hechos que sean de interés general, puede dar lugar a videos o fotografías de personas sobre las que difícilmente sea posible obtener su consentimiento.<sup>28</sup>

La normativa trae un principio de solución al caso apuntado anteriormente, ya que en un principio aquello llevaría a reflexionar que quien desarrolla una actividad fotográfica o de filmación sujeta registración de la base de dato, cuando captura imágenes de personas situadas en los ámbitos geográficos en los que circunstancialmente desarrolla su actividad debería eliminar esas imágenes si no obtiene la conformidad de la persona implicada. Todo lo cual haría que sea imposible la práctica profesional que lleva adelante.

---

<sup>28</sup> Si se piensa que los VANT's circundan el espacio aéreo obteniendo filmaciones o fotografías de forma indeterminada, ha de existir una gran cantidad de población afectada por esta actividad a la que no es posible solicitarle un consentimiento previo. Se ha llegado al extremo –sobre lo que no coincide- de afirmarse que "Un padre podría usar un dron con su hijo en la playa. Pero no debe haber personas en el medio. Y si fotografía o filma a terceros sin consentimiento, estará en infracción". (según ejemplifica SCHINCA Fabián, jefe del Departamento de Normativa Aeronáutica, Normas y Procedimientos Internos de la ANAC. – Recuperado el 8 de nov. de 2015. <http://www.udesa.edu.ar/medios/crece-la-polemica-por-el-uso-recreativo-de-los-drones-y-se-viene-una-regulacion#sthash.iHaDOOHp.dpuf>).

A los fines de subsanar de algún modo la dificultad apuntada el artículo 4 prevé para la captura de datos que tenga por finalidad la realización de estudios científicos, cartográficos, sobre recursos naturales, medio ambiente o actividades análogas que no tengan por objeto la recolección de datos personales, que se aplique sobre la imagen de la persona, en el más breve lapso que las reglas del arte lo permitan, una técnica de disociación definitiva (por ejemplo difuminación de la imagen). Lo cierto es que en ocasiones las imágenes son parte del paisaje o del objetivo de la filmación o fotografía profesional o científica sin ser determinantes ni protagonistas. Una toma audiovisual que pretenda demostrar la densidad demográfica de un determinado sitio de una ciudad no podría presumirse en ella la existencia de un interés general para su conocimiento y difusión al pública –artículo 1-, y ciertamente la difuminación de las imágenes de las personas haría perder todo sentido a la captura de la imagen, además de hacer de ella un desastre estético. En el sentido de la regulación, siendo que de esa imagen podría surgir un dato personal situado fuera de las circunstancias puntuales de excepción, cabría aplicar esta regulación.

### **El uso privado de los datos**

Más allá de lo establecido en la Disposición 20/2015 y en los Artículos 5 y 6 antes referidos, debe atenderse a otra condición que posee la Ley 25.326 para definir que se está frente a una base de datos sujeta a registración. Ello es su utilización fuera del ámbito privado de la persona titular del archivo o de la base de datos.

Cabe indagar esta circunstancia en la que es posible que la actividad llevada a cabo por un VANT pueda ser ajena a la ley 25.326. La incursión en el espacio aéreo y la capacidad de no ser detectables en sí mismas no implican la existencia de una base de datos destinada a dar informes si es que es de uso exclusivo de la persona que la posee. Si ello fuera de otro modo, implicaría la necesidad de registrar todo tipo de aparato fotográfico o audiovisual que sea portado en cualquier aeronave tripulada por seres humanos, o bien lisa y llanamente cualquier archivo de una cámara fotográfica o video filmadora. Y en modo alguno puede considerarse que un video o fotografía que no se encuentra sujeto a cesión a terceros ni excede el uso personal de quien la detenta, puede encontrarse bajo esta reglamentación.

Tampoco será necesario el permiso de aquellas personas cuya imagen o voz haya sido capturada por un VANT cuando los datos se recolecten con motivo de la realización de un evento privado en los que el registro audiovisual responda a usos y costumbres establecidos (casamientos, cumpleaños y otras fiestas). Ello, mientras lo que haya sido capturado de forma audiovisual no represente una violación a la intimidad debido a estar capturada en circunstancias fuera del propio ámbito festivo en el que se esté desarrollando. La normativa refiere puntualmente a una “intromisión desproporcionada en la privacidad del titular del datos” lo cual nos lleva a la reflexión respecto a si una imagen capturada en un aparte del lugar central donde se está desarrollando el evento puede llegar a ser ilegal. Deberá evaluarse en el caso el alcance del término “intromisión desproporcionada”. Ante estas circunstancias la

actividad de los denominados “*Paparazzi*” se encuentra en riesgo de ser considerada ilícita en cualquier circunstancia.

### **La actividad del Estado Nacional en el ejercicio de sus funciones**

La actividad estatal dentro de sus facultades policiales se encuentra exenta de las regulaciones impuestas por la Disposición. Siendo coherente con lo dispuesto en la ley 25.326, tampoco necesitará permiso el Estado Nacional cuando use VANT’s en el ejercicio de sus funciones ni cuando los datos se recolecten “con motivo de la atención a personas en situaciones de emergencia o siniestros”. De tal forma, el Estado Nacional (no así los estados provinciales ni municipales) tiene libertad de uso de los VANT’s con solamente justificar algún tipo de necesidad pública.

El uso de los VANT’s como medios para prevenir delitos sin duda alguna significa un avance que la tecnología suministra a los estados. Lamentablemente y sin fundamento alguno se ha dejado afuera de esta exención a los estados provinciales y municipales quienes tienen a su cargo la seguridad pública. Con esta exclusión se coloca a estos poderes constitucionales en una situación de debilidad, provocando seguramente un conflicto en cuanto a la aplicación territorial de esta restricción, ya que constituyendo el Poder de Policía una atribución inherente a los tres niveles de gobierno vigentes en el sistema federal argentino, es lógico que los gobiernos provinciales y municipales –dentro de sus competencias- se consideren legitimados para utilizar los VANT’s como medios efectivos para prevenir la inseguridad pública. Esta reglamentación de la autoridad nacional discrimina innecesariamente y seguramente será objeto de impugnaciones si es que la DNPDP pretende imponer la normativa a los gobiernos locales.

En orden al uso de las imágenes captadas por el Estado Nacional mediante VANT’s, cabe alertar que no cualquier captura se encuentra exenta de la reglamentación. Únicamente es posible darle tratamiento sin consentimiento de la persona titular del dato a aquellas imágenes que surgen de una actividad lícita y necesaria para la actividad público estatal. Es imperativo que el tratamiento de estos datos sea limitado al objetivo deseado legalmente y encuentre en sus Responsables una discreción tal que no permita una violación innecesaria de la intimidad de las personas. La policía y las demás autoridades pública deben cuidar extremadamente de invadir los derechos y libertades de las personas e interferir con los derechos al respeto de la vida privada y a la protección de los datos personales amparados en el artículo 12 de la Declaración Universal de Derechos Humanos,<sup>29</sup> el artículo 17 del Pacto

---

<sup>29</sup> Artículo 12: “Nadie será objeto de injerencias arbitrarias en su vida privada, ni su familia, ni cualquier entidad, ni de ataques a su honra o su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques”.

Internacional de Derechos Civiles y Políticos,<sup>30</sup> artículo 11 del Pacto de San José de Costa Rica.<sup>31</sup> De este modo, la actividad estatal siempre deberá estar vinculada a una necesidad legal y únicamente si es necesario y realmente cumple con el objetivo de interés público y la necesidad de proteger los derechos y libertades de las personas. Será necesaria utilizar los VANT's enmarcados en los conceptos de necesidad y proporcionalidad y protección de datos conforme los indica la normativa.

Será indicativo de un buen uso de los VANT's como instrumento de seguridad o interés estatal que no exista ningún otro medio menos invasivo de la intimidad personal para recolectar los datos que se pretende tratar y se vean limitados a los supuestos e necesidad del tratamiento (Vg. Proteger la seguridad de las personas o recabar información durante una investigación criminal).

Como directa derivación de lo expuesto, los datos colectados por VANT's no deberían ser usados para efectuar vigilancias no ordenadas por la Justicia ni para el trazado de perfiles personales ni para realizar análisis fuera del objeto puntual de la captación de los datos bajo tratamiento. Es necesario que el uso de los VANT's por parte del Estado no sea generalizado, debiendo ser utilizados restrictivamente. Por lo tanto, sólo deben usarse con fines estrictamente detallados y justificados. Que sean fijados anticipada y motivadamente. Siendo recomendable que su uso se vea limitado geográfica y temporalmente.

De un modo contrario a las recomendaciones europeas del GT29, la Disposición permite, sin limitación alguna, el uso de VANT's durante un acto público. Ello podría aparejar que mediante la excusa de dar seguridad pública o ejecutar alguna actividad profesional, comercial o científica, se pretenda perseguir a una determinada persona sin siquiera poseer orden judicial o alguna otra razón dentro del ejercicio lícito de la actividad estatal que lo permita, invadiendo de esta forma su intimidad. Bastaría nada más hacer volar un VANT's sobre un acto público pero enfocando disimuladamente a la persona espiada para excusarse en la ausencia de consentimiento. Es peligroso y habrá que estar muy atentos a su debida utilización, que el Estado Nacional posee esta herramienta de investigación, mucho más en nuestro país donde existen numerosos y renombrados antecedentes de violación a los deberes de confidencialidad en las investigaciones policiales.

---

<sup>30</sup> Artículo 17: "1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación; 2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques."

<sup>31</sup> Artículo 11:"1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad; 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación; 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques".

## **El uso en una propiedad privada**

Quien use un VANT dentro de una propiedad privada tampoco necesitará permiso para registrar imágenes. De todas formas se recomienda la restricción máxima de la recolección de datos. Al mismo tiempo se dispone que el Responsable del tratamiento deberá prever mecanismos razonables para que los asistentes se informen de que pueden ser captados por una VANT.

Sin embargo, cuando se trate de un espacio de ingreso habitual de público, se deberá informar sobre el uso de VANT's para filmar. La distinción se encuentra dada entre la utilización en la propiedad privada de uso exclusivo y la que se desarrolle en una propiedad privada pero de acceso público, como podría ser un club o una centro de salud. Los términos en que se deberá en los términos del artículo 6° de la Ley N° 25.326, por tanto deberá el Responsable del tratamiento indicar: a) La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios; b) La existencia del archivo, registro, banco de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable; c) El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos referidos en el artículo siguiente; d) Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos; e) La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos.

## **El uso para fines científicos y similares**

Por otra parte, la disposición establece que cuando se recolecten datos con VANT's para fines científicos, cartográficos, sobre recursos naturales, medio ambiente o actividades análogas que no tengan por objeto la recolección de datos personales, pero que por razones técnicas, dicha recolección no pueda evitarse, se deberá aplicar sobre dichos datos personales en el más breve lapso que las reglas del arte lo permitan una "técnica de disociación definitiva", por ejemplo, la "difuminación" de la imagen de modo que no permita identificar a persona alguna.

En este supuesto el principio general es la permisión de la actividad de los VANT's. La única restricción está dada por la captura de datos personales de modo indirecto. Lo cual podría darse en el supuesto que durante el vuelo que sirve para captar las imágenes deseadas por el Responsable del tratamiento, se capture una imagen o un audio que afecte la intimidad de la persona por tratarse de una recuperación en la que pueda ser detectada de manera concreta un dato personal de ella.

## **La utilización meramente recreativa**

La Disposición da un tratamiento particular al registro de imágenes durante el uso recreativo de un VANT. El artículo 5° de la Disposición 20/2015: "no se aplicarán

las disposiciones de la presente reglamentación cuando se utilicen VANT's o drones con fines exclusivamente recreativos y sin la finalidad de capturar datos personales de terceros". Para estos casos, sin embargo, la norma dicta una serie de "recomendaciones que deberán adoptarse" las que se encuentran desarrolladas en su Anexo II.

En estas recomendaciones se indica que "el uso recreativo de VANT's o drones deberá hacerse teniendo en consideración las implicancias que tiene su uso sobre la privacidad de las personas, debiendo dar un uso prudencial al mismo, evitando la observación, entrometimiento o molestia en la vida y actividades de terceros", señala la nueva norma.

Si durante el uso recreativo de un VANT incidentalmente se recolectase información de carácter personal y el titular del dato se manifiesta en contra, el operador del VANT deberá tomar los recaudos necesarios para evitar dicha recolección, y en caso de haber ya recolectado las imágenes, deberá eliminarlas. En este punto, la disposición aclara que esto vale aún en espacios públicos. Aquí la duda está en cómo obtener la conformidad y si ante la falta de esta, aquel que solamente usa la información para uso exclusivo personal debe eliminarla de todas formas. En este último caso, no se aprecia cuál sería el bien jurídico tutelado.

A la vez, el operador del VANT deberá evitar acceder a lugares que impliquen un riesgo para la intimidad de las personas, como ser ventanas, jardines, terrazas o cualquier otro espacio de una propiedad privada cuyo acceso no le fuere previamente autorizado.

También deberá tenerse especial cuidado de no recolectar datos íntimos o de carácter sensible (aquellos que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual). "Por esta razón –dice la norma–, deberá evitarse la captura de información personal mediante el VANT o dron en establecimientos de la salud, lugares de culto, manifestaciones políticas o sindicales, y en aquellos lugares donde se pueda presumir la preferencia sexual de las personas, entre otros".

## **Conclusión**

En conclusión, la Disposición viene a reglamentar el uso de esta tecnología robótica que encuentra en la actualidad una multiplicidad de usos, desde los meramente recreativos hasta los científicos o de seguridad nacional. Todo ello de forma algo redundante si lo consideramos desde el puntual ángulo del tratamiento de datos, ya que para se encuentra la reglamentación que la ley 25.326 contiene para todo tipo de base de datos sin importar el método de captura.

Por su parte, la Disposición hace hincapié en el particular riesgo a la privacidad que implica el uso de los VANT's, mientras no se ha experimentado regulación alguna sobre los numerosos vehículos móviles que de una u otra forma pueden contribuir a la captación de datos personales.

A primera vista, esta norma está restringiendo el uso de estos aparatos de avanzada tecnología partiendo quizás de una premisa equivocada: la utilidad de esta tecnología en sí misma no es distinta a un vehículo aéreo o terrestre a control remoto como los que hace tiempo existen en el mercado, o bien otro tipo de vehículos tripulados por seres humanos. La captación de imágenes mediante el uso de esos vehículos, en principio, no requiere consentimiento previo y solamente se verá sujeta a reproche legal si es usado en desmedro de la intimidad de las personas. Ello conforme las normas civiles actualmente vigentes. Claro está que, si conformasen una base de datos, por la normativa general, también son pasibles de registración.

El límite natural a este tipo de tecnologías al servicio del ser humano es la libertad individual de quien puede resultar afectado y por supuesto su intimidad. En cuanto a las responsabilidades que pudieren haber por el uso indebido de los VANT's, debe mencionarse que las normas civiles establecen el suficiente reproche legal ante conductas que ocasionen perjuicios a las personas cuya intimidad se vea violentada por el uso de VANT. En esos supuestos, como en todo orden del derecho privado será el particular damnificado quien deba o no instar el reclamo correspondiente.

La Disposición contiene restricciones a las libertades civiles, las que en la medida que no violen espacios de seguridad nacional o la intimidad de otras personas, no debieran ser objeto de reglamentación. Como toda regulación, excede el ámbito de aplicación que surge de las normas de mayor rango y por otra parte discrimina entre iguales. En tal sentido, la diferencia que dispone entre el Estado Nacional y los provinciales y municipales denota una inconsistencia que seguramente deberá ser resuelta en el futuro.

En nuestra opinión, crear normas que prevean casos especiales dentro de aquellos que ya poseen reglamentación general, en pos de regular la conducta humana bajo el pretexto de prevenir eventuales intromisiones a la privacidad de las personas, es propia de los estados dirigistas que buscan controlar las acciones humanas lícitas de la sociedad política que gobiernan, bajo la apariencia de darle a esas mismas personas que dicen proteger un alto grado de cuidado paternalista. La intimidad es la contracara de la libertad y a la vez es complementaria. En la materia que analizamos resulta ser la contracara porque a mayor resguardo de la intimidad de las personas, menor es la libertad de tomar imágenes de estas, aun cuando no se encuentren estrictamente en un ámbito íntimo. Más luego, es complementaria porque el respeto a la intimidad de una persona implica concederle la libertad de elegir cuándo y cómo mostrarse públicamente y de concederle el resguardo legal acorde para que dentro de un determinado espacio ella pueda proteger su imagen respecto de personas con las que no desea compartirla.

En la medida que este tipo de normativas limiten su ámbito de injerencia a precisar un listado de operadores habituales de VANT's podrá constituir una herramienta de prevención adecuada. Ahora bien, cuando el regulador avanza hacia una restricción que implica intervenir en los archivos de imágenes de aquellos responsables del tratamiento de datos, disponiendo por caso, trámites burocráticos ineficientes para el contralor que se pretende hacer, o abusa de sus facultades regulatorias a fin de tomar mayor control sobre la actividad lícita de los ciudadanos, es la libertad personal la que se vería peligrosamente amenazada. Entonces de suceder que la reglamentación termina avanzando sobre los derechos de las personas en relación a su libertad de tránsito, expresión, contratación, etc., es muy probable que deba ser revisada en el futuro. Es que en modo alguno puede ser sustentable en el tiempo una norma que bajo el prisma de pretender resguardar los datos personales de las personas, acceda a controlar de modo irrazonable la libertad civil.

### **Bibliografía:**

VASSALLO, Carlos María. "Aeronaves sin piloto (Drones)" publicado por Editorial La Ley el 24 de octubre de 2014.

Agencia Española de Protección de Datos. Recuperado el 8 de noviembre de 2015.

[http://www.agpd.es/portalwebAGPD/internacional/Proteccion\\_datos\\_mundo/index-ides-idphp.php](http://www.agpd.es/portalwebAGPD/internacional/Proteccion_datos_mundo/index-ides-idphp.php)

Dirección Nacional de Datos Personales. Recuperado el 8 de noviembre de 2015. <http://www.jus.gob.ar/datos-personales/cumpli-con-la-ley/%C2%BFcuales-son-tus-obligaciones.aspx>

COLOM José Luis. Blog Aspectos profesionales: Protección de Datos, Cloud Computing y Sistemas de Gestión. Editor: Recuperado el 15 de Nov. de 2015. <http://www.aspectosprofesionales.info/2015/06/dictamen-012015-sobre-la-privacidad-y.html>

Grupo de trabajo del Artículo 29 de la Comisión Europea. Dictamen 01/2015 sobre la privacidad y la protección de datos en relación con la utilización de aviones no tripulados(drones), [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp231\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp231_en.pdf)