



La consulta plantea la conformidad con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal (LOPD), y su Reglamento de desarrollo, aprobado por Real Decreto 1720/2007, de 21 de diciembre (RDLOPD) y restante normativa aplicable, al uso de dispositivos particulares que permitan captación de imágenes o videos por parte de los miembros de las Fuerzas y Cuerpos de Seguridad.

I

De conformidad con los artículos 1 y 2.1 LOPD, la normativa que nos ocupa tiene por objeto la protección de los datos de carácter personal como derecho fundamental, definiéndose el concepto de dato de carácter personal en el apartado a) del artículo 3 de la LOPD, como *“Cualquier información concerniente a personas físicas identificadas o identificables”*. La imagen de una persona es un dato personal, considerando también el artículo 5.1. f) RDLOPD, que como tales *“Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, concerniente a personas físicas identificadas o identificables”*. Y en este mismo sentido el Considerando 14 de la Directiva 95/46/CE que señala *“(14) Considerando que, habida cuenta de la importancia que, en el marco de la sociedad de la información, reviste el actual desarrollo de las técnicas para captar, transmitir, manejar, registrar, conservar o comunicar los datos relativos a las personas físicas constituidos por sonido e imagen, la presente Directiva habrá de aplicarse a los tratamientos que afectan a dichos datos;”*.

Por su parte, el artículo 3 de la LOPD define en su letra c) el tratamiento de datos como aquellas *“operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias”*. De acuerdo con esta definición de tratamiento de datos personales, la captación y en su caso grabación de imágenes de las personas

constituye un tratamiento de datos personales incluido en el ámbito de aplicación de la normativa citada.

En este mismo sentido se pronuncia la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.

En segundo lugar, tal y como indica la consulta, debe señalarse que la Ley Orgánica 4/1997, de 4 agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos, señala en su artículo 1.1 que *“la presente Ley regula la utilización por las Fuerzas y Cuerpos de Seguridad de videocámaras para grabar imágenes y sonidos en lugares públicos, abiertos o cerrados, y su posterior tratamiento, a fin de contribuir a asegurar la convivencia ciudadana, la erradicación de la violencia y la utilización pacífica de las vías y espacios públicos, así como de prevenir la comisión de delitos, faltas e infracciones relacionados con la seguridad pública”*.

El artículo 5 de la citada Ley Orgánica establece los requisitos para la autorización de videocámaras móviles, disponiendo lo siguiente:

“1. En las vías o lugares públicos donde se haya autorizado la instalación de videocámaras fijas, podrán utilizarse simultáneamente otras de carácter móvil para el mejor cumplimiento de los fines previstos en esta Ley, quedando, en todo caso, supeditada la toma, que ha de ser conjunta, de imagen y sonido, a la concurrencia de un peligro concreto y demás requisitos exigidos en el artículo 6.

2. También podrán utilizarse en los restantes lugares públicos videocámaras móviles. La autorización de dicho uso corresponderá al máximo responsable provincial de las Fuerzas y Cuerpos de Seguridad quien atenderá a la naturaleza de los eventuales hechos susceptibles de filmación, adecuando la utilización del medio a los principios previstos en el artículo 6.

La resolución motivada que se dicte autorizando el uso de videocámaras móviles se pondrá en conocimiento de la Comisión prevista en el artículo 3 en el plazo máximo de setenta y dos horas, la cual podrá recabar el



soporte físico de la grabación a efectos de emitir el correspondiente informe.

En casos excepcionales de urgencia máxima o de imposibilidad de obtener a tiempo la autorización indicada en razón del momento de producción de los hechos o de las circunstancias concurrentes, se podrán obtener imágenes y sonidos con videocámaras móviles, dando cuenta, en el plazo de setenta y dos horas, mediante un informe motivado, al máximo responsable provincial de las Fuerzas y Cuerpos de Seguridad y a la Comisión aludida en el párrafo anterior, la cual, si lo estima oportuno, podrá requerir la entrega del soporte físico original y emitir el correspondiente informe.

En el supuesto de que los informes de la Comisión previstos en los dos párrafos anteriores fueran negativos, la autoridad encargada de la custodia de la grabación procederá a su destrucción inmediata.

3. La Comisión prevista en el artículo 3 será informada quincenalmente de la utilización que se haga de videocámaras móviles y podrá recabar en todo momento el soporte de las correspondientes grabaciones y emitir un informe al respecto.

4. En el caso de que las autoridades competentes aludidas en esta Ley lo consideren oportuno, se podrá interesar informe de la Comisión prevista en el artículo 3 sobre la adecuación de cualquier registro de imágenes y sonidos obtenidos mediante videocámaras móviles a los principios del artículo 6.”

Además, el artículo 6 establece los principios que deberán regir esa autorización, estableciendo que:

“1. La utilización de videocámaras estará presidida por el principio de proporcionalidad, en su doble versión de idoneidad y de intervención mínima.

2. La idoneidad determina que sólo podrá emplearse la videocámara cuando resulte adecuado, en una situación concreta, para el mantenimiento de la seguridad ciudadana, de conformidad con lo dispuesto en esta Ley.



3. La intervención mínima exige la ponderación, en cada caso, entre la finalidad pretendida y la posible afectación por la utilización de la videocámara al derecho al honor, a la propia imagen y a la intimidad de las personas.

4. La utilización de videocámaras exigirá la existencia de un razonable riesgo para la seguridad ciudadana, en el caso de las fijas, o de un peligro concreto, en el caso de las móviles.

5. No se podrán utilizar videocámaras para tomar imágenes ni sonidos del interior de las viviendas, ni de sus vestíbulos, salvo consentimiento del titular o autorización judicial, ni de los lugares incluidos en el artículo 1 de esta Ley cuando se afecte de forma directa y grave a la intimidad de las personas, así como tampoco para grabar conversaciones de naturaleza estrictamente privada. Las imágenes y sonidos obtenidos accidentalmente en estos casos deberán ser destruidas inmediatamente, por quien tenga la responsabilidad de su custodia.”

Asimismo el artículo 7 de dicha norma regula los aspectos procedimentales disponiendo que:

“1. Realizada la filmación de acuerdo con los requisitos establecidos en la Ley, si la grabación captara la comisión de hechos que pudieran ser constitutivos de ilícitos penales, las Fuerzas y Cuerpos de Seguridad pondrán la cinta o soporte original de las imágenes y sonidos en su integridad a disposición judicial con la mayor inmediatez posible y, en todo caso, en el plazo máximo de setenta y dos horas desde su grabación. De no poder redactarse el atestado en tal plazo, se relatarán verbalmente los hechos a la autoridad judicial, o al Ministerio Fiscal, junto con la entrega de la grabación.

2. Si la grabación captara hechos que pudieran ser constitutivos de infracciones administrativas relacionadas con la seguridad ciudadana, se remitirán al órgano competente, igualmente de inmediato, para el inicio del oportuno procedimiento sancionador.”

Por tanto, tal y como hemos indicado en ocasiones anteriores, como en informe de 31 de julio de 2012, no corresponde a esta Agencia determinar si resulta conforme a la citada Ley Orgánica la instalación de los dispositivos citados, debiendo someterse dicha autorización a los requisitos señalados en el artículo 5 y cumplir con los principios establecidos en el artículo 6, si bien

partiendo en todo caso de la excepcionalidad de la medida que se contempla en dichas normas.

II

La cuestión planteada en esta consulta ya ha sido atendida por esta Agencia, en el sentido de entender que los dispositivos particulares de los miembros de las Fuerzas y Cuerpos de Seguridad no cumplirían, con carácter general, los requisitos generales expuestos en el apartado anterior del presente informe. Así, en informe de 30 de octubre de 2015 estudiamos el supuesto de que la policía local pudiera captar imágenes por dispositivos particulares – si bien realizando funciones de policía judicial, las conclusiones son plenamente aplicables - y señalamos que, en principio y con carácter general, no cumpliría con las medidas de seguridad exigibles:

“En lo que respecta a la aplicación de la normativa de protección de datos al supuesto planteado, debe tenerse en cuenta que la Ley Orgánica 15/1999 exige a los responsables de los ficheros o tratamientos la adopción de las correspondientes medidas de seguridad disponiendo a este respecto su artículo 9.1 que “El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.”

El número 2 de dicho precepto prohíbe el registro de datos de carácter personal en ficheros “que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.”

Debe, además, recordarse que, como ha señalado reiteradamente la Audiencia Nacional en sus sentencias (por todas ellas SAN de 6-10-2011), la seguridad constituye una obligación de resultado consistente en que se adopten las medidas necesarias para evitar que los datos se pierdan, extravíen o acaben en manos de terceros.

Por tanto, debe examinarse si tales cámaras domésticas y teléfonos móviles pueden garantizar la seguridad de los datos de forma que no se

produzcan pérdidas o alteraciones de los datos y, muy especialmente, dada la generalización de uso de dispositivos inteligentes, la posibilidad de acceso por terceros a los datos en ellas almacenados. Debe así tenerse en cuenta que puede producirse inadvertidamente una cesión de datos a terceros, definida en el artículo 3 i) de la Ley Orgánica 15/1999 como “Toda revelación de datos realizada a una persona distinta del interesado”. Este riesgo se produce, por ejemplo, si se instalan aplicaciones en los teléfonos móviles que requieran el acceso a los datos obrantes en las mismas o cuando se produce un almacenamiento de las imágenes o de su copia en una nube (produciéndose así una comunicación de datos al proveedor del servicio de cloud computing), con el agravante de que en ocasiones la falta de transparencia de los desarrolladores de aplicaciones no permite conocer si se están produciendo accesos a los datos almacenados en los dispositivos.

Teniendo en cuenta los riesgos señalados debe considerarse que el uso de cámaras o móviles personales de los agentes no garantiza la seguridad de los datos, en tanto que los usos privados que cada agente pueda realizar con sus propios dispositivos no resultan compatibles con las medidas de seguridad que para el ejercicio de las funciones de policía judicial deben adoptarse por los responsables del fichero policial del que formarán parte tales grabaciones.

Asimismo, en el caso de que se utilizasen dispositivos inteligentes que se hayan entregado con carácter oficial para su uso con fines policiales, éstos deberán responder a las exigencias de lo establecido en el artículo 9 de la Ley Orgánica 15/1999, debiendo, en particular, adoptarse todas las precauciones para impedir accesos indebidos a los datos que con ellos se capten”.