



La consulta plantea en esencia la posibilidad de utilización de los teléfonos particulares de los policías para el envío telemático de fotografías de las personas a quienes se intenta identificar en la calle en virtud de la Ley de protección de la seguridad ciudadana, pero carecen de documentación en ese momento, sin consentimiento de estos, a la Comisaría correspondiente para de ese modo proceder telemáticamente a su identificación y evitar al ciudadano tener que acudir a Comisaría para ser identificado.

Pues bien, hay que decir que estas mismas cuestiones, esto es, la utilización de aparatos particulares de miembros de las Fuerzas y Cuerpos de Seguridad del Estado para la realización de actividades de captación o grabación de imágenes en el ejercicio de su actividad oficial ha sido objeto de reiterados informes de esta agencia cuya doctrina por lo tanto habrá que seguir.

Con carácter general debe indicarse que los artículos 1 y 2 de la Ley Orgánica 15/1999, de Protección de datos de Carácter Personal (LOPD) extienden su protección a los derechos de los ciudadanos en lo que se refiere al tratamiento de sus datos de carácter personal, siendo definidos éstos en el artículo 3.a) de la citada Ley como *“cualquier información concerniente a personas físicas identificadas o identificables.”* El artículo 5.1 del Reglamento de desarrollo de la Ley Orgánica 15/1999, aprobado por Real Decreto 1720/2007, de 21 de diciembre, (RLOPD) precisa que constituye un dato de carácter personal *“Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.”* En consecuencia, la imagen de una persona identificada o identificable constituye un dato de carácter personal, por lo que su tratamiento está sujeto a lo previsto en la normativa de protección de datos.

Debe así tenerse en cuenta que tanto la captación en vivo como la grabación de dichos datos o cualquier otro concerniente a personas identificadas o identificables constituyen un tratamiento de datos de carácter personal, tal y como dispone el artículo 3 de la Ley Orgánica 15/1999 al definir éste como *“las 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.” En aplicación de la normativa de protección de datos, para que dicho tratamiento de datos sea lícito será preciso que se encuentre legitimado en la forma prevista en el artículo 6 de la Ley Orgánica 15/1999 conforme al cual “el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa.”

La cuestión planteada en esta consulta, como se ha expresado anteriormente, 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 requeridos por la normativa de protección de datos. 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”.

En consecuencia, ninguna de las dos actuaciones planteadas en la consulta por el consultante, ambas realizadas a través de teléfonos móviles particulares de los policías individualmente considerados, se considera compatible con la legislación de protección de datos.

AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS



AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS



Gabinete Jurídico