PRIVACIDAD VERSUS LUCHA CONTRA LA DELINCUENCIA: LAS AUTORIDADES PUEDEN TENER ACCESO A LOS DATOS GENERADOS POR UN TELÉFONO MÓVIL SIN QUE SE TRATE DE DELITOS ESPECIALMENTE GRAVES*

STJUE de 2 de octubre 2018 (asunto C-207/16)

Iuliana Raluca Stroie**
Centro de Estudios de Consumo
Universidad de Castilla-La Mancha

Fecha de publicación: 10 de octubre de 2018

El TJUE declara en la Sentencia de 2 de octubre de 2018 que el acceso de las autoridades públicas a los datos personales protegidos por los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea puede estar justificado por la prevención, investigación, descubrimiento y persecución de delitos "en general" sin necesidad de que se trate de delincuencia "grave". No obstante, la gravedad de la injerencia a dichos derechos fundamentales debe guardar proporcionalidad con la gravedad de los delitos que se intentan prevenir, investigar, descubrir o perseguir.

El litigio principal que dio lugar a la cuestión prejudicial se refiere a una investigación policial que se realizó como consecuencia de un robo con violencia de una cartera y un teléfono móvil. La Policía Judicial española solicitó al Juzgado de Instrucción que le concediera acceso a los números de teléfono activados, por un período de doce días desde la fecha del robo, con el código IMEI del teléfono móvil sustraído, los datos personales o de filiación de los titulares o usuarios de los números de teléfono correspondientes a las tarjetas SIM activadas con dicho código, como su nombre, apellidos y, en su caso, dirección.

El Juzgado denegó dicha diligencia al considerar que la misma no era idónea para identificar a los autores del delito y, por considerar que los hechos investigados no

* Trabajo realizado en el marco del Proyecto Convenio de colaboración entre la UCLM y el Ilustre Colegio Notarial De Castilla-La Mancha (17 enero 2014) (OBSV) con referencia CONV140025, que dirige el Prof. Ángel Carrasco Perera.
** ORCID ID: 0000-0003-1998-5412

constituyan delitos graves (sancionados con una pena de prisión superior a cinco años). Conforme a la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, la cesión de los datos conservados por las operadoras de telefonía está limitada a la investigación de delitos graves.

El Ministerio Fiscal recurrió esta decisión alegando que, por la naturaleza de los hechos y habida cuenta de una sentencia del Tribunal Supremo, de 26 de julio de 2010, relativa a un caso similar, debería haberse acordado la cesión de los datos en cuestión.

En base a una modificación de la Ley de Enjuiciamiento Criminal posterior al auto recurrido en apelación, que introdujo dos nuevos criterios alternativos para determinar el nivel de gravedad de un delito, el Tribunal remitente, pregunta al TJUE si dicho umbral de gravedad se ha de determinar en función de la pena prevista para castigar el delito o, si es necesario, además, identificar en la conducta delictiva particulares niveles de lesividad para bienes jurídicos individuales y/o colectivos. Además, si la determinación de la gravedad del delito se realiza en base a la pena imponible, conforme ha declarado el TJUE en su sentencia de 8 de abril de 2014 [Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238], cuál debería ser ese umbral mínimo y si sería compatible con una previsión general de límite en tres años de prisión (conforme establece la legislación española con posterioridad a la modificación antes mencionada).

El TJUE señala que el acceso de las autoridades públicas a los datos conservados por los proveedores de servicios de comunicaciones electrónicas constituye en todo caso "una injerencia en el derecho fundamental al respeto de la vida privada, consagrado en el artículo 7 de la Carta, incluso a falta de circunstancias que permitan calificar esta injerencia de «grave» y sin que sea relevante que la información relativa a la vida privada de que se trate tenga o no carácter sensible o que los interesados hayan sufrido o no inconvenientes en razón de tal injerencia" y, también constituye una injerencia en el derecho fundamental a la protección de los datos personales garantizado por el artículo 8 de la Carta. No obstante, una norma nacional que regula el acceso de las autoridades públicas a estos datos, estableciendo por tanto, una excepción al principio de confidencialidad de las comunicaciones electrónicas, puede ser justificada si cumple estrictamente alguno de los objetivos recogidos en el art. 15, apartado 1 de la Directiva 2002/58. Uno de los objetivos recogidos en el mentado precepto se refiere textualmente a la *prevención, investigación, descubrimiento y persecución de delitos* sin especificar si estos han de ser graves o no.

Conforme a la interpretación del TJUE en su sentencia de 21 de diciembre de 2016 (Asunto Tele2 Sverige y Watson y otros), *solo la lucha contra la delincuencia grave podría justificar un acceso a datos personales conservados por los proveedores de*

servicios de comunicaciones electrónicas que, considerados en su conjunto, permitan extraer conclusiones precisas sobre la vida privada de las personas cuyos datos han sido conservados. Pero el Tribunal procede a matizar esta interpretación, señalando que el objetivo perseguido por una norma que regula este acceso debe guardar relación con la gravedad de la injerencia en los derechos fundamentales en cuestión. Es decir, una injerencia grave en los derechos fundamentales debe tener como objetivo la lucha contra la delincuencia que a su vez esté también calificada de «grave» y, por el contrario, cuando la injerencia que implica dicho acceso no es grave, puede estar justificada por el objetivo de prevenir, investigar, descubrir y perseguir «delitos» en general.

Por ello, lo que se ha de dilucidar en el presente caso es si la injerencia de la Policía Judicial española en los derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta pueda considerarse en este caso grave. En este sentido, se ha de tener en cuenta que los datos a los que se solicita acceso se limitan a la tarjeta o tarjetas SIM activadas con el teléfono móvil sustraído y los datos personales o de filiación de los titulares de estas tarjetas SIM, en un determinado plazo (12 días), sin que de los mismos se puedan extraer conclusiones precisas sobre la vida privada de las personas cuyos datos se ven afectados. Con lo cual no se trataría de una injerencia grave en los derechos fundamentales de las personas afectadas y la misma *estaría justificada por el objetivo de prevenir, investigar, descubrir y perseguir «delitos» en general, sin que sea necesario que dichos delitos estén calificados como «graves».*