



Los delitos que no revistan particular gravedad pueden justificar el acceso a los datos personales almacenados por proveedores de servicios de comunicaciones electrónicas cuando dicho acceso no suponga una injerencia grave en la vida privada

En el marco de la investigación de un robo con violencia de una cartera y un teléfono móvil, la Policía Judicial española solicitó al Juzgado de Instrucción encargado del caso que le concediera acceso a los datos personales o de filiación de los usuarios de los números de teléfono activados desde el teléfono sustraído durante un período de doce días desde la fecha del robo. El juez instructor denegó la diligencia solicitada, en particular porque consideraba que los hechos que habían dado lugar a la investigación penal no constituían delito «grave» —es decir, con arreglo al Derecho español, los delitos sancionados con una pena de prisión superior a cinco años—, único tipo de delitos que permite justificar el acceso a los datos personales o de filiación.¹ El Ministerio Fiscal interpuso recurso de apelación contra dicha decisión ante la Audiencia Provincial de Tarragona.

La Directiva sobre la privacidad y las comunicaciones electrónicas² establece que los Estados miembros pueden limitar los derechos de los ciudadanos cuando tal limitación constituya una medida necesaria, proporcionada y apropiada en una sociedad democrática para proteger la seguridad nacional, la defensa y la seguridad pública, o garantizar la prevención, investigación, descubrimiento y persecución de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas.

La Audiencia Provincial de Tarragona expone que, con posterioridad a la adopción de la decisión del juez instructor, el legislador español introdujo³ dos criterios alternativos para determinar el nivel de gravedad de un delito respecto del cual se autoriza la conservación y la cesión de los datos personales. El primero es un criterio material, vinculado a delitos específicos y graves, especialmente lesivos para los intereses jurídicos individuales y colectivos. El segundo es un criterio normativo-formal que establece un umbral mínimo de tres años de prisión, umbral que abarca la gran mayoría de los delitos. Además, el tribunal español observa que el interés del Estado en castigar las conductas infractoras no puede justificar injerencias desproporcionadas en los derechos fundamentales consagrados en la Carta de los Derechos Fundamentales de la Unión Europea («Carta»). Por tanto, la Audiencia Provincial de Tarragona pregunta al Tribunal de Justicia acerca de la fijación del umbral de gravedad de los delitos a partir del cual puede justificarse una injerencia en los derechos fundamentales, como el acceso por parte de las

¹ Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones (BOE n.º 251, de 19 de octubre de 2007, p. 42517).

² Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) (DO 2002, L 201, p. 37), en su versión modificada por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009 (DO 2009, L 337, p. 11).

³ Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica (BOE n.º 239, de 6 de octubre de 2015, p. 90192).

autoridades nacionales competentes a los datos personales almacenados por los proveedores de servicios de comunicaciones electrónicas.

Mediante su sentencia dictada hoy, el Tribunal de Justicia recuerda que el acceso de las autoridades públicas a datos personales almacenados por los proveedores de servicios de comunicaciones electrónicas en el marco de un procedimiento de instrucción penal está incluido en el ámbito de aplicación de la Directiva. Además, el acceso a los datos que permiten identificar a los titulares de las tarjetas SIM activadas con un teléfono móvil sustraído, como los nombres, los apellidos y, en su caso, las direcciones de dichos titulares, constituye una injerencia en los derechos fundamentales de éstos, consagrados en la Carta. No obstante, el Tribunal de Justicia declara que esta injerencia no presenta una gravedad tal que, en el ámbito de la prevención, investigación, descubrimiento y persecución de delitos, dicho acceso deba limitarse a la lucha contra la delincuencia grave.

El Tribunal de Justicia señala que el acceso de las autoridades públicas a datos almacenados por los proveedores de servicios de comunicaciones electrónicas constituye una injerencia en los derechos fundamentales al respeto de la vida privada y a la protección de datos, consagrados en 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 dicha injerencia. Sin embargo, la Directiva enumera objetivos que pueden justificar una norma nacional que regule el acceso de las autoridades públicas a estos datos y establezca de ese modo una excepción al principio de confidencialidad de las comunicaciones electrónicas. Esta enumeración tiene carácter exhaustivo, por lo que dicho acceso ha de responder efectiva y estrictamente a uno de esos objetivos. El Tribunal de Justicia observa a este respecto que **el tenor de la Directiva no limita el objetivo de la prevención, investigación, descubrimiento y persecución de delitos a la lucha contra los delitos graves, sino que se refiere a los «delitos» en general.**

En su sentencia *Tele2 Sverige*,⁴ el Tribunal de Justicia declaró que únicamente la lucha contra la criminalidad grave puede justificar el acceso de las autoridades públicas a datos almacenados por los proveedores de servicios de comunicaciones electrónicas que, examinados en su conjunto, permitan extraer conclusiones precisas sobre la vida privada de las personas cuyos datos se ven afectados. No obstante, esa interpretación estaba motivada por el hecho de que el objetivo perseguido por una norma que regula ese acceso debe guardar relación con la gravedad de la injerencia en los derechos fundamentales en cuestión que suponga dicha operación. En efecto, conforme al principio de proporcionalidad, una injerencia grave sólo puede estar justificada en este ámbito por el objetivo de luchar contra la delincuencia que a su vez también deba calificarse de «grave». **En cambio, cuando la injerencia no es grave, dicho acceso puede estar justificado por el objetivo de prevenir, investigar, descubrir y perseguir «delitos» en general.**

El Tribunal de Justicia considera que **el acceso limitado únicamente a los datos cubiertos por la solicitud de que se trata no puede calificarse de injerencia «grave» en los derechos fundamentales de los individuos cuyos datos se ven afectados, ya que dichos datos no permiten extraer conclusiones precisas sobre su vida privada.** El Tribunal de Justicia deduce de ello que **la injerencia que supone el acceso a esos datos puede estar justificada por el objetivo de prevenir, investigar, descubrir y perseguir «delitos» en general, sin que sea necesario que dichos delitos sean calificados de «graves».**

NOTA: La remisión prejudicial permite que los tribunales de los Estados miembros, en el contexto de un litigio del que estén conociendo, interroguen al Tribunal de Justicia acerca de la interpretación del Derecho de la Unión o sobre la validez de un acto de la Unión. El Tribunal de Justicia no resuelve el litigio nacional, y es el tribunal nacional quien debe resolver el litigio de conformidad con la decisión del Tribunal de Justicia. Dicha decisión vincula igualmente a los demás tribunales nacionales que conozcan de un problema similar.

Documento no oficial, destinado a los medios de comunicación y que no vincula al Tribunal de Justicia.

⁴ Sentencia de 21 de diciembre de 2016, *Tele2 Sverige y Watson y otros* (C-203/15 y C-698/15, véase el CP nº 145/16).

El [texto íntegro](#) de la sentencia se publica en el sitio CURIA el día de su pronunciamiento

Contactos con la prensa: Cristina López Roca ☎ (+352) 4303 3667

Las imágenes del pronunciamiento de la sentencia se encuentran disponibles en
«[Europe by Satellite](#)» ☎ (+32) 2 2964106