



El Abogado General Saugmandsgaard Øe propone al Tribunal de Justicia que declare que incluso los delitos que no son de una gravedad particular pueden justificar un acceso a los metadatos básicos de las comunicaciones electrónicas, siempre que ese acceso no afecte gravemente a la vida privada

En el marco de la investigación de un robo con violencia de una cartera y de un teléfono móvil, la Policía Judicial española solicitó al Juzgado de Instrucción 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 Juzgado de Instrucción denegó esta solicitud, fundamentando en particular su decisión en que los hechos en que se basaba la investigación penal no eran constitutivos de delito «grave» (es decir, conforme al Derecho español, una infracción castigada con una pena de prisión superior a cinco años), único tipo de delito que permite justificar en España el acceso a los datos personales o de filiación.¹ El Ministerio Fiscal interpuso recurso contra esta decisión ante la Audiencia Provincial de Tarragona.

La Directiva sobre la privacidad y las comunicaciones electrónicas² establece que los Estados miembros podrán 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, la seguridad pública, o la prevención, investigación, descubrimiento y persecución de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas.

En sus sentencias *Digital Rights*³ y *Tele2 Sverige*,⁴ el Tribunal de Justicia utilizó el concepto de «delitos graves» para apreciar la legitimidad y la proporcionalidad de una injerencia en el derecho al respeto de la vida privada y familiar y en el derecho a la protección de los datos personales, derechos que están consagrados en la Carta de los Derechos Fundamentales de la Unión Europea.

¹ Ley 25/2007 de 18 de octubre de 2007, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones (BOE núm. 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 Sentencia de 8 de abril de 2014, *Digital Rights Ireland y Seitlinger y otros* (C-293/12 y C-594/12, véase el CP n.º 54/14). En esta sentencia, el Tribunal de Justicia declaró la invalidez de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE (DO 2006, L 105, p. 54).

⁴ Sentencia de 21 de diciembre de 2016, *Tele2 Sverige y Watson y otros* (C-203/15 y C-698/15, véase el CP n.º 145/16). En esta sentencia, el Tribunal de Justicia declaró que el Derecho de la Unión se opone, *por una parte*, «a una normativa nacional que establece, con la finalidad de luchar contra la delincuencia, la conservación generalizada e indiferenciada de todos los datos de tráfico y de localización de todos los abonados y usuarios registrados en relación con todos los medios de comunicación electrónica» y, *por otra*, «a una normativa nacional que regula la protección y la seguridad de los datos de tráfico y de localización, en particular el acceso de las autoridades nacionales competentes a los datos conservados, sin limitar dicho acceso, en el marco de la lucha contra la delincuencia, a los casos de delincuencia grave, sin supeditar dicho acceso a un control previo por un órgano jurisdiccional o una autoridad administrativa independiente, y sin exigir que los datos de que se trata se conserven en el territorio de la Unión».

La Audiencia Provincial de Tarragona señala que, tras la adopción de la decisión del Juzgado de Instrucción, el legislador español introdujo ⁵ dos criterios alternativos para determinar el umbral de gravedad de un delito para cuya investigación se autoriza la conservación y la cesión de los datos personales. El primero es un criterio material identificado con el terrorismo y los delitos cometidos en el seno de una organización criminal. El segundo es un criterio normativo-formal que establece un umbral mínimo de tres años de prisión. El tribunal español subraya que dicho umbral abarca la gran mayoría de los tipos penales. 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, a la luz de las sentencias citadas, puede estar justificada la restricción de los derechos fundamentales cuando las autoridades nacionales competentes acceden a los datos personales conservados por los proveedores de servicios de comunicaciones electrónicas.

En sus conclusiones presentadas hoy, el Abogado General Henrik Saugmandsgaard Øe señala en primer lugar que una medida como la solicitada por la Policía Judicial en el presente caso constituye una injerencia en el derecho al respeto de la vida privada y familiar y en el derecho a la protección de los datos personales. Sin embargo, a juicio del Abogado General, **en las sentencias Digital Rights y Tele2, el Tribunal de Justicia estableció una correlación entre la gravedad de la injerencia observada y la gravedad de la razón que permite justificarla.** Así pues, para exigir que, en la fase de la justificación de la injerencia, exista un «delito grave» que permita establecer una excepción al principio de confidencialidad de las comunicaciones electrónicas, es necesario que **la injerencia sea grave. Según el Abogado General, en el presente caso falta este elemento esencial.**

El Abogado General añade que la naturaleza de la injerencia controvertida en el presente asunto es distinta de las injerencias examinadas en las dos sentencias citadas. **En efecto, se trata de una medida limitada** que tiene por objeto la posibilidad de acceso, por parte de las autoridades competentes y para llevar a cabo la investigación de un delito, a datos conservados con fines comerciales por los prestadores de servicios, y que se refiere únicamente a la identidad (nombre, apellidos y en su caso la dirección) de una categoría restringida de abonados o usuarios de un medio de comunicación específico, esto es, aquellos cuyo número de teléfono haya sido activado desde el teléfono móvil cuya sustracción es objeto de la investigación, **y durante un período limitado** -doce días. **El Abogado General considera que los efectos potencialmente perjudiciales para las personas a las que se refiere la solicitud de acceso controvertida son a la vez moderados y limitados**, habida cuenta de que no se trata de divulgar los datos solicitados al público en general y de que la facultad de acceso concedida a las autoridades policiales está acompañada de garantías procesales, ya que lleva consigo un control judicial. **Por consiguiente, la injerencia que entraña la comunicación de estos datos personales o de filiación no reviste un carácter particularmente grave**, dado que, en esas circunstancias concretas, los datos de esta naturaleza no afectan directamente ni en gran medida a la vida privada de las personas afectadas.

El Abogado General indica que, según la Directiva, una excepción al principio de confidencialidad de las comunicaciones electrónicas puede estar justificada por el objetivo de interés general de prevención y persecución de los *delitos*, sin realizar precisión alguna en cuanto a su naturaleza. Por tanto, no es imperativo que los delitos que legitiman la medida restrictiva de que se trata puedan calificarse de «graves» en el sentido de las sentencias Digital Rights y Tele2. Según el Abogado General, **sólo cuando la injerencia es particularmente grave las infracciones que pueden justificar una injerencia de este tipo deben ser, a su vez, de una particular gravedad. En cambio, en el supuesto de una injerencia leve (esto es, cuando los datos cuya comunicación se solicita no afecten gravemente a la vida privada), incluso los delitos que no tienen una particular gravedad pueden justificar tal injerencia (es decir, el acceso a los datos solicitados).**

⁵ Ley Orgánica 13/2015 de 5 de octubre de 2015, 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 núm. 239, de 6 de octubre de 2015, p. 90192).

En particular, el Abogado General considera que el **Derecho de la Unión no se opone a que las autoridades competentes puedan acceder a los datos personales o de filiación en poder de los proveedores de servicios de comunicaciones electrónicas que permitan encontrar a los supuestos autores de un delito que no revista carácter grave. El Abogado General concluye que, a la luz de la Directiva, la medida solicitada por la Policía Judicial en el presente caso implica una injerencia en los derechos fundamentales garantizados por la Directiva y por la Carta que no alcanza un nivel de gravedad suficiente para que dicho acceso deba reservarse a los casos en que el delito sea grave.**

NOTA: Las conclusiones del Abogado General no vinculan al Tribunal de Justicia. La función del Abogado General consiste en proponer al Tribunal de Justicia, con absoluta independencia, una solución jurídica al asunto del que se ocupa. Los jueces del Tribunal de Justicia comienzan ahora sus deliberaciones sobre este asunto. La sentencia se dictará en un momento posterior.

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.

El [texto íntegro](#) de las conclusiones se publica en el sitio CURIA el día de su lectura

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

*Las imágenes de la lectura de las conclusiones se encuentran disponibles en
«[Europe by Satellite](#)» ☎ (+32) 2 2964106*