SENTENCIA DEL TRIBUNAL DE JUSTICIA (Gran Sala)

de 2 de octubre de 2018 (*)

«Procedimiento prejudicial — Comunicaciones electrónicas — Tratamiento de datos personales — Directiva 2002/58/CE — Artículos 1 y 3 — Ámbito de aplicación — Confidencialidad de las comunicaciones electrónicas — Protección — Artículos 5 y 15, apartado 1 — Carta de los Derechos Fundamentales de la Unión Europea — Artículos 7 y 8 — Datos tratados en el marco de la prestación de servicios de comunicaciones electrónicas — Acceso de las autoridades nacionales a los datos para la investigación de un delito — Umbral de gravedad del delito que puede justificar el acceso a los datos»

En el asunto C−207/16,

que tiene por objeto una petición de decisión prejudicial planteada, con arreglo al artículo 267 TFUE, por la Audiencia Provincial de Tarragona, mediante auto de 6 de abril de 2016, recibido en el Tribunal de Justicia el 14 de abril de 2016, en el procedimiento incoado por

Ministerio Fiscal,

EL TRIBUNAL DE JUSTICIA (Gran Sala),

integrado por el Sr. K. Lenaerts, Presidente, el Sr. A. Tizzano, Vicepresidente, la Sra. R. Silva de Lapuerta y los Sres. T. von Danwitz (Ponente), J.L. da Cruz Vilaça, C.G. Fernlund y C. Vajda, Presidentes de Sala, y los Sres. E. Juhász y A. Borg Barthet, la Sra. C. Toader, los Sres. M. Safjan y D. Šváby, la Sra. Berger y los Sres. E. Jarašiūnas y E. Regan, Jueces;

Abogado General: Sr. H. Saugmandsgaard Øe;

Secretario: Sra. L. Carrasco Marco, administradora;

habiendo considerado los escritos obrantes en autos y celebrada la vista el 29 de enero de 2018;

consideradas las observaciones presentadas:

– en nombre del Ministerio Fiscal, por la Sra. E. Tejada de la Fuente;

– en nombre del Gobierno español, por el Sr. M.A. Sampol Pucurull, en calidad de agente;

– en nombre del Gobierno checo, por los Sres. M. Smolek y J. Vláčil y la Sra. A. Brabcová, en calidad de agentes;

– en nombre del Gobierno danés, por el Sr. J. Nymann-Lindegren y la Sra. M.S. Wolff, en calidad de agentes;

– en nombre del Gobierno estonio, por la Sra. N. Grünberg, en calidad de agente;

– en nombre de Irlanda, por las Sras. M. Browne, L. Williams y E. Creedon y el Sr. A. Joyce, en calidad de agentes, asistidos por la Sra. E. Gibson, BL;

– en nombre del Gobierno francés, por el Sr. D. Colas y las Sras. E. de Moustier y E. Armoet, en calidad de agentes;

– en nombre del Gobierno letón, por las Sras. I. Kucina y J. Davidoviča, en calidad de agentes;

– en nombre del Gobierno húngaro, por los Sres. M.Z. Fehér y G. Koós, en calidad de agentes;

– en nombre del Gobierno austriaco, por la Sra. C. Pesendorfer, en calidad de agente;

– en nombre del Gobierno polaco, por el Sr. B. Majczyna y las Sras. D. Lutostańska y J. Sawicka, en calidad de agentes;

– en nombre del Gobierno del Reino Unido, por el Sr. S. Brandon y la Sra. C. Brodie, en calidad de agentes, asistidos por el Sr. C. Knight, Barrister, y por el Sr. G. Facenna, QC;

– en nombre de la Comisión Europea, por las Sras. M.I. Martínez del Peral y P. Costa de Oliveira y los Sres. R. Troosters y D. Nardi, en calidad de agentes;

oídas las conclusiones del Abogado General, presentadas en audiencia pública el 3 de mayo de 2018;

dicta la siguiente

Sentencia

1 La petición de decisión prejudicial tiene por objeto, en esencia, la interpretación del artículo 15, apartado 1, de la 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) (en lo sucesivo, «Directiva 2002/58»), en relación con los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, «Carta»).

2 Dicha petición se ha presentado en el marco de un recurso interpuesto por el Ministerio Fiscal contra la resolución del Juzgado de Instrucción n.º 3 de Tarragona (en lo sucesivo, «juez instructor») relativa a la denegación de acceso de la Policía Judicial a datos personales almacenados por proveedores de servicios de comunicaciones electrónicas.

Marco jurídico

Derecho de la Unión

Directiva 95/46

3 A tenor del artículo 2, letra b), de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO 1995, L 281, p. 31), procede entender, a efectos de esta última, por «tratamiento de datos personales», «cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción».

4 El artículo 3 de dicha Directiva, titulado «Ámbito de aplicación», establece:

«1. Las disposiciones de la presente Directiva se aplicarán al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.

2. Las disposiciones de la presente Directiva no se aplicarán al tratamiento de datos personales:

– efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, como las previstas por las disposiciones de los títulos V y VI del Tratado de la Unión Europea y, en cualquier caso, al tratamiento de datos que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando

dicho tratamiento esté relacionado con la seguridad del Estado) y las actividades del Estado en materia penal;

– efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas.»

Directiva 2002/58

5 Los considerandos 2, 11, 15 y 21 de la Directiva 2002/58 enuncian lo siguiente:

«(2) La presente Directiva pretende garantizar el respeto de los derechos fundamentales y observa los principios consagrados, en particular, en la [Carta]. Señaladamente, la presente Directiva pretende garantizar el pleno respeto de los derechos enunciados en los artículos 7 y 8 de [esta].

[...]

(11) Al igual que la Directiva [95/46], la presente Directiva no aborda la protección de los derechos y las libertades fundamentales en relación con las actividades no regidas por el Derecho comunitario. Por lo tanto, no altera el equilibrio actual entre el derecho de las personas a la intimidad y la posibilidad de que disponen los Estados miembros, según se indica en el apartado 1 del artículo 15 de la presente Directiva, de tomar las medidas necesarias para la protección de la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando las actividades tengan relación con asuntos de seguridad del Estado) y la aplicación del Derecho penal. En consecuencia, la presente Directiva no afecta a la capacidad de los Estados miembros para interceptar legalmente las comunicaciones electrónicas o tomar otras medidas, cuando sea necesario, para cualquiera de estos fines y de conformidad con el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, según la interpretación que se hace de este en las sentencias del Tribunal Europeo de Derechos Humanos. Dichas medidas deberán ser necesarias en una sociedad democrática y rigurosamente proporcionales al fin que se pretende alcanzar y deben estar sujetas, además, a salvaguardias adecuadas, de conformidad con el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales.

[...]

(15) Una comunicación puede incluir cualquier dato relativo a nombres, números o direcciones facilitado por el remitente de una comunicación o el usuario de una conexión para llevar a cabo la comunicación. Los datos de tráfico pueden incluir cualquier conversión de dicha información efectuada por la red a través de la cual se transmita la comunicación a efectos de llevar a cabo la transmisión. [...]

[...]

(21) Deben adoptarse medidas para evitar el acceso no autorizado a las comunicaciones a fin de proteger la confidencialidad de las mismas, incluidos tanto sus contenidos como cualquier dato relacionado con ellas, por medio de las redes públicas de comunicaciones y los servicios de comunicaciones electrónicas disponibles al público. La legislación nacional de algunos Estados miembros prohíbe solamente el acceso intencionado no autorizado a las comunicaciones.»

6 El artículo 1 de la Directiva 2002/58, titulado «Ámbito de aplicación y objetivo», dispone:

«1. La presente Directiva establece la armonización de las disposiciones nacionales necesaria para garantizar un nivel equivalente de protección de las libertades y los derechos fundamentales y, en particular, del derecho a la intimidad y la confidencialidad, en lo que respecta al tratamiento de los datos personales en el sector de las comunicaciones electrónicas, así como la libre circulación de tales datos y de los equipos y servicios de comunicaciones electrónicas en la Comunidad.

2. Las disposiciones de la presente Directiva especifican y completan la Directiva [95/46] a los efectos mencionados en el apartado 1. Además, protegen los intereses legítimos de los abonados que

sean personas jurídicas.

3. La presente Directiva no se aplicará a las actividades no comprendidas en el ámbito de aplicación del Tratado constitutivo de la Comunidad Europea, como las reguladas por las disposiciones de los títulos V y VI del Tratado de la Unión Europea, ni, en cualquier caso, a las actividades que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dichas actividades estén relacionadas con la seguridad del mismo) y a las actividades del Estado en materia penal.»

7 A tenor del artículo 2 de la Directiva 2002/58, titulado «Definiciones»:

«Salvo disposición en contrario, serán de aplicación a efectos de la presente Directiva las definiciones que figuran en la Directiva [95/46] y en la Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas (Directiva marco) [(DO 2002, L 108, p. 33)].

Además, a efectos de la presente Directiva se entenderá por:

[...]

b) “datos de tráfico”: cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de la facturación de la misma;

c) “datos de localización”: cualquier dato tratado en una red de comunicaciones electrónicas o por un servicio de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público;

d) “comunicación”: cualquier información intercambiada o conducida entre un número finito de interesados por medio de un servicio de comunicaciones electrónicas disponible para el público. No se incluye en la presente definición la información conducida, como parte de un servicio de radiodifusión al público, a través de una red de comunicaciones electrónicas, excepto en la medida en que la información pueda relacionarse con el abonado o usuario identificable que reciba la información;

[...]».

8 El artículo 3 de la Directiva 2002/58, titulado «Servicios afectados», establece:

«La presente Directiva se aplicará al tratamiento de datos personales en relación con la prestación de servicios de comunicaciones electrónicas disponibles al público en las redes públicas de comunicaciones de la Comunidad, incluidas las redes públicas de comunicaciones que den soporte a dispositivos de identificación y recopilación de datos.»

9 Conforme al artículo 5 de la Directiva 2002/58, titulado «Confidencialidad de las comunicaciones»:

«1. Los Estados miembros garantizarán, a través de la legislación nacional, la confidencialidad de las comunicaciones, y de los datos de tráfico asociados a ellas, realizadas a través de las redes públicas de comunicaciones y de los servicios de comunicaciones electrónicas disponibles al público. En particular, prohibirán la escucha, la grabación, el almacenamiento u otros tipos de intervención o vigilancia de las comunicaciones y los datos de tráfico asociados a ellas por personas distintas de los usuarios, sin el consentimiento de los usuarios interesados, salvo cuando dichas personas estén autorizadas legalmente a hacerlo de conformidad con el apartado 1 del artículo 15. [...]

[...]

3. Los Estados miembros velarán por que únicamente se permita el almacenamiento de información, o la obtención de acceso a la información ya almacenada, en el equipo terminal de un abonado o usuario, a condición de que dicho abonado o usuario haya dado su consentimiento después de que se le

haya facilitado información clara y completa, en particular sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Directiva [95/46]. [...]»

10 El artículo 6 de la Directiva 2002/58, con el epígrafe «Datos de tráfico», dispone:

«1. Sin perjuicio de lo dispuesto en los apartados 2, 3 y 5 del presente artículo y en el apartado 1 del artículo 15, los datos de tráfico relacionados con abonados y usuarios que sean tratados y almacenados por el proveedor de una red pública de comunicaciones o de un servicio de comunicaciones electrónicas disponible al público deberán eliminarse o hacerse anónimos cuando ya no sea necesario a los efectos de la transmisión de una comunicación.

2. Podrán ser tratados los datos de tráfico necesarios a efectos de la facturación de los abonados y los pagos de las interconexiones. Se autorizará este tratamiento únicamente hasta la expiración del plazo durante el cual pueda impugnarse legalmente la factura o exigirse el pago.

[...]»

11 El artículo 15 de la mencionada Directiva, titulado «Aplicación de determinadas disposiciones de la Directiva [95/46]», establece en su apartado 1:

«Los Estados miembros podrán adoptar medidas legales para limitar el alcance de los derechos y las obligaciones que se establecen en los artículos 5 y 6, en los apartados 1 a 4 del artículo 8 y en el artículo 9 de la presente Directiva, cuando tal limitación constituya una medida necesaria proporcionada y apropiada en una sociedad democrática para proteger la seguridad nacional (es decir, la seguridad del Estado), la defensa, la seguridad pública, o la prevención, investigación, descubrimiento y persecución de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas a que se hace referencia en el apartado 1 del artículo 13 de la Directiva [95/46]. Para ello, los Estados miembros podrán adoptar, entre otras, medidas legislativas en virtud de las cuales los datos se conserven durante un plazo limitado justificado por los motivos establecidos en el presente apartado. Todas las medidas contempladas en el presente apartado deberán ser conformes con los principios generales del Derecho comunitario, incluidos los mencionados en los apartados 1 y 2 del artículo 6 del Tratado de la Unión Europea.»

Derecho español

Ley 25/2007

12 El artículo 1 de la 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), dispone:

«1. Esta Ley tiene por objeto la regulación de la obligación de los operadores de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación, así como el deber de cesión de dichos datos a los agentes facultados siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales.

2. Esta Ley se aplicará a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o usuario registrado.

[...]»

Código Penal

13 El artículo 13, apartado 1, de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal (Código Penal) (BOE n.º 281, de 24 de noviembre de 1995, p. 33987), está redactado en los siguientes términos:

«Son delitos graves las infracciones que la Ley castiga con pena grave.»

14 El artículo 33 de dicho Código establece lo siguiente:

«1. En función de su naturaleza y duración, las penas se clasifican en graves, menos graves y leves.

2. Son penas graves:

a) La prisión permanente revisable.

b) La prisión superior a cinco años.

[...]»

Ley de Enjuiciamiento Criminal

15 Con posterioridad a los hechos del litigio principal, la Ley de Enjuiciamiento Criminal ha sido modificada por la 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).

16 Dicha Ley, que entró en vigor el 6 de diciembre de 2015, introduce en la Ley de Enjuiciamiento Criminal la cuestión del acceso a los datos relativos a las comunicaciones telefónicas y telemáticas conservados por los proveedores de servicios de comunicaciones electrónicas.

17 El artículo 579, apartado 1, de la Ley de Enjuiciamiento Criminal, en su versión resultante de la Ley Orgánica 13/2015, dispone:

«1. El juez podrá acordar la detención de la correspondencia privada, postal y telegráfica, incluidos faxes, burofaxes y giros, que el investigado remita o reciba, así como su apertura o examen, si hubiera indicios de obtener por estos medios el descubrimiento o la comprobación [de] algún hecho o circunstancia relevante para la causa, siempre que la investigación tenga por objeto alguno de los siguientes delitos:

1.º Delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión.

2.º Delitos cometidos en el seno de un grupo u organización criminal.

3.º Delitos de terrorismo.

[...]»

18 El artículo 588 ter j de dicho Código establece lo siguiente:

«1. Los datos electrónicos conservados por los prestadores de servicios o personas que faciliten la comunicación en cumplimiento de la legislación sobre retención de datos relativos a las comunicaciones electrónicas o por propia iniciativa por motivos comerciales o de otra índole y que se encuentren vinculados a procesos de comunicación, solo podrán ser cedidos para su incorporación al proceso con autorización judicial.

2. Cuando el conocimiento de esos datos resulte indispensable para la investigación, se solicitará del juez competente autorización para recabar la información que conste en los archivos automatizados de los prestadores de servicios, incluida la búsqueda entrecruzada o inteligente de datos, siempre que se precisen la naturaleza de los datos que hayan de ser conocidos y las razones que justifican la cesión.»

Procedimiento principal y cuestiones planteadas

19 El Sr. Hernández Sierra presentó una denuncia ante la Policía por un robo con violencia, cometido el 16 de febrero de 2015, durante el cual resultó herido y le sustrajeron la cartera y el teléfono móvil.

20 El 27 de febrero de 2015, la Policía Judicial presentó un oficio ante el juez instructor solicitando que se ordenase a diversos proveedores de servicios de comunicaciones electrónicas la transmisión de los números de teléfono activados, desde el 16 de febrero hasta el 27 de febrero de 2015, con el código relativo a la identidad internacional del equipo móvil (en lo sucesivo, «código IMEI») del teléfono móvil sustraído, así como 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.

21 Mediante auto de 5 de mayo de 2015, el juez instructor denegó la diligencia solicitada. Por un lado, consideró que esta no era idónea para identificar a los autores del delito. Por otra parte, denegó la solicitud porque la Ley 25/2007 limitaba la cesión de los datos conservados por las operadoras de telefonía a los delitos graves. Con arreglo al Código Penal, los delitos graves son los sancionados con una pena de prisión superior a cinco años, mientras que los hechos presuntos no parecían ser constitutivos de delito grave.

22 El Ministerio Fiscal interpuso recurso de apelación contra dicho auto ante el tribunal remitente, alegando que, dada 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 de que se trata.

23 El tribunal remitente expone que, con posterioridad a dicho auto, el legislador español modificó la Ley de Enjuiciamiento Criminal mediante la aprobación de la Ley Orgánica 13/2015. Esta Ley, que es pertinente para la resolución del recurso principal, introdujo dos nuevos criterios alternativos para determinar el nivel de gravedad de un delito. Se trata, por un lado, de un estándar material identificado por conductas típicas de particular y grave relevancia criminógena que incorporan particulares tasas de lesividad para bienes jurídicos individuales y colectivos. Por otro, el legislador nacional ha introducido un criterio normativo-formal basado en la pena prevista para el delito de que se trate. No obstante, el umbral de tres años de prisión que establece abarca la gran mayoría de los delitos. Además, el tribunal remitente observa que el interés del Estado en castigar las conductas infractoras no puede justificar injerencias desproporcionadas en los derechos fundamentales consagrados en la Carta.

24 A este respecto, el tribunal remitente considera que, en el procedimiento principal, las Directivas 95/46 y 2002/58 establecen el vínculo de conexión con la Carta. Por tanto, la normativa nacional controvertida en el litigio principal está incluida en el ámbito de aplicación de la Carta, con arreglo al artículo 51, apartado 1, de esta, a pesar de que la sentencia de 8 de abril de 2014, Digital Rights Ireland y otros (C−293/12 y C−594/12, EU:C:2014:238) 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).

25 El tribunal remitente afirma que, en dicha sentencia, el Tribunal de Justicia reconoció que la conservación y cesión de datos de tráfico constituyen injerencias especialmente graves en los derechos garantizados por los artículos 7 y 8 de la Carta e identificó los criterios de apreciación del respeto del principio de proporcionalidad, entre ellos la gravedad de los delitos que justifican la conservación de estos datos y el acceso a ellos para la investigación de un delito.

26 En estas circunstancias, la Audiencia Provincial de Tarragona decidió suspender el procedimiento y plantear al Tribunal de Justicia las siguientes cuestiones prejudiciales:

«1) ¿La suficiente gravedad de los delitos como criterio que justifica la injerencia en los derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta puede identificarse únicamente en atención a la pena que pueda imponerse al delito que se investiga o es necesario, además, identificar en la conducta delictiva particulares niveles de lesividad para bienes jurídicos individuales y/o colectivos?

2) En su caso, si se ajustara a los principios constitucionales de la Unión, utilizados por el [Tribunal de Justicia] 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] como estándares de control estricto de la Directiva, la determinación de la gravedad del delito atendiendo solo a la pena imponible ¿cuál debería ser ese umbral mínimo? ¿Sería compatible con una previsión general de límite en tres años de prisión?»

Procedimiento ante el Tribunal de Justicia

27 Mediante decisión del Presidente del Tribunal de Justicia de 23 de mayo de 2016, el procedimiento ante el Tribunal de Justicia se suspendió hasta que se dictase sentencia en los asuntos acumulados Tele2 Sverige y Watson y otros, C−203/15 y C−698/15 (sentencia de 21 de diciembre de 2016, EU:C:2016:970; en lo sucesivo, «sentencia Tele2 Sverige y Watson y otros»). A raíz del pronunciamiento de dicha sentencia, se preguntó al tribunal remitente si deseaba mantener o retirar su petición de decisión prejudicial. En respuesta, el tribunal remitente, mediante escrito de 30 de enero de 2017, recibido en el Tribunal de Justicia el 14 de febrero de 2017, hizo saber que consideraba que dicha sentencia no le permitía analizar, con suficiente certeza la normativa nacional controvertida en el litigio principal a la luz del Derecho de la Unión. Como consecuencia, el procedimiento ante el Tribunal de Justicia se reanudó el 16 de febrero de 2017.

Sobre las cuestiones prejudiciales

28 El Gobierno español alega, por una parte, que el Tribunal de Justicia es incompetente para responder a la petición de decisión prejudicial y, por otra, que esta es inadmisible.

Sobre la competencia del Tribunal de Justicia

29 En sus observaciones escritas presentadas al Tribunal de Justicia, el Gobierno español manifestó la opinión, a la que se adhirió el Gobierno del Reino Unido en la vista, de que el Tribunal de Justicia no es competente para responder a la petición de decisión prejudicial debido a que, con arreglo al artículo 3, apartado 2, primer guion, de la Directiva 95/46 y al artículo 1, apartado 3, de la Directiva 2002/58, el litigio principal está excluido del ámbito de aplicación de esas dos Directivas. Por lo tanto, a su juicio el presente asunto no está comprendido en el ámbito de aplicación del Derecho de la Unión, de modo que la Carta, en virtud de su propio artículo 51, apartado 1, no es aplicable.

30 Según el Gobierno español, es cierto que el Tribunal de Justicia ha declarado, en la sentencia Tele2 Sverige y Watson y otros que una medida legal que regula el acceso de las autoridades nacionales a los datos conservados por los proveedores de servicios de comunicaciones electrónicas está incluida en el ámbito de aplicación de la Directiva 2002/58. No obstante, en el caso de autos se trata de una solicitud de acceso de una autoridad pública en virtud de una resolución judicial dictada en el marco de un procedimiento de instrucción penal, a datos personales conservados por los proveedores de servicios de comunicaciones electrónicas. El Gobierno español deduce de ello que esta solicitud de acceso se inscribe en el ejercicio del ius puniendi por las autoridades nacionales, de modo que forma parte de la actividad del Estado en materia penal, incluida en la excepción prevista en el artículo 3, apartado 2, primer guion, de la Directiva 95/46 y el artículo 1, apartado 3, de la Directiva 2002/58.

31 Para analizar esta excepción de incompetencia, debe señalarse que el artículo 1, apartado 1, de la Directiva 2002/58 dispone que dicha Directiva prevé la armonización de las disposiciones nacionales necesarias para, entre otras cuestiones, garantizar un nivel equivalente de protección de las libertades y los derechos fundamentales, en particular del derecho a la intimidad y a la confidencialidad, en lo que respecta al tratamiento de los datos personales en el sector de las comunicaciones electrónicas. Con arreglo a su artículo 1, apartado 2, dicha Directiva especifica y completa la Directiva 95/46 a los efectos mencionados en el citado apartado 1.

32 El artículo 1, apartado 3, de la Directiva 2002/58 excluye de su ámbito de aplicación las «actividades del Estado» en los sectores que enumera, entre las que figuran las actividades del Estado en materia penal y las que tengan por objeto la seguridad pública, la defensa y la seguridad del Estado, incluido el bienestar económico del Estado cuando dichas actividades estén relacionadas con la seguridad del mismo (sentencia Tele2 Sverige y Watson y otros, apartado 69 y jurisprudencia citada). Las actividades enumeradas en dicho apartado a título de ejemplo son, en todos los casos, actividades propias del

Estado o de las autoridades estatales y ajenas a la esfera de actividades de los particulares (véase, por analogía, en relación con el artículo 3, apartado 2, primer guion, de la Directiva 95/46, la sentencia de 10 de julio de 2018, Jehovan Todistajat, C−25/17, EU:C:2018:551, apartado 38 y jurisprudencia citada).

33 En cuanto al artículo 3 de la Directiva 2002/58, este enuncia que dicha Directiva se aplicará al tratamiento de datos personales en relación con la prestación de servicios de comunicaciones electrónicas disponibles al público en las redes públicas de comunicaciones de la Unión, incluidas las redes públicas de comunicaciones que den soporte a dispositivos de identificación y recopilación de datos (en lo sucesivo, «servicios de comunicaciones electrónicas»). Por tanto, debe considerarse que la citada Directiva regula las actividades de los proveedores de tales servicios (sentencia Tele2 Sverige y Watson y otros, apartado 70).

34 En lo que atañe al artículo 15, apartado 1, de la Directiva 2002/58, el Tribunal de Justicia ya ha declarado que las medidas legales contempladas en esa disposición están incluidas en el ámbito de aplicación de la Directiva, aun si se refieren a actividades propias de los Estados o las autoridades estatales, ajenas a los ámbitos de actividad de los particulares, e incluso si las finalidades a las que deben responder tales medidas coinciden en esencia con las finalidades que persiguen las actividades mencionadas en el artículo 1, apartado 3, de la Directiva 2002/58. En efecto, el artículo 15, apartado 1, de esa Directiva presupone necesariamente que las medidas nacionales que se establecen en ella están incluidas en el ámbito de aplicación de la citada Directiva, ya que esta solo autoriza expresamente a los Estados miembros a adoptarlas cumpliendo los requisitos que establece. Por otro lado, las medidas legales a que se refiere el artículo 15, apartado 1, de la Directiva 2002/58 regulan, a los efectos mencionados en dicha disposición, la actividad de los proveedores de servicios de comunicaciones electrónicas (véase, en este sentido, la sentencia Tele2 Sverige y Watson y otros, apartados 72 a 74).

35 El Tribunal de Justicia ha concluido que el mencionado artículo 15, apartado 1, de la Directiva 2002/58, en relación con su artículo 3, debe interpretarse en el sentido de que están incluidas en el ámbito de aplicación de dicha Directiva no solo una medida legislativa que obliga a los proveedores de servicios de comunicaciones electrónicas a conservar los datos de tráfico y los datos de localización, sino también una medida legislativa relativa al acceso de las autoridades nacionales a los datos conservados por dichos proveedores (véase, en este sentido, la sentencia Tele2 Sverige y Watson y otros, apartados 75 y 76).

36 En efecto, la protección de la confidencialidad de las comunicaciones electrónicas y de sus datos de tráfico, garantizada en el artículo 5, apartado 1, de la Directiva 2002/58, se aplica a las medidas adoptadas por todas las personas distintas de los usuarios, ya sean personas físicas o entidades privadas o públicas. Como confirma el considerando 21 de dicha Directiva, esta tiene como objetivo evitar «[todo] acceso» no autorizado a las comunicaciones, incluido «todo dato relativo a esas comunicaciones», para proteger la confidencialidad de las comunicaciones electrónicas (véase, en este sentido, la sentencia Tele2 Sverige y Watson y otros, apartado 77).

37 Ha de añadirse que las medidas legales que obligan a los proveedores de servicios de comunicaciones electrónicas a conservar datos personales o conceder a las autoridades nacionales competentes el acceso a estos datos implican necesariamente un tratamiento de dichos datos por esos proveedores (véase, en este sentido, la sentencia Tele2 Sverige y Watson y otros, apartados 75 y 78). Por tanto, tales medidas, en la medida en que regulan las actividades de dichos proveedores, no pueden asimilarse a actividades propias de los Estados, mencionadas en el artículo 1, apartado 3, de la Directiva 2002/58.

38 En el presente asunto, como se desprende del auto de remisión, la solicitud controvertida en el litigio principal, por la que la Policía Judicial solicita autorización judicial para acceder a datos personales conservados por proveedores de servicios de comunicaciones electrónicas, tiene como fundamento la Ley 25/2007, en relación con la Ley de Enjuiciamiento Criminal, en su versión aplicable a los hechos del litigio principal, que regula el acceso de las autoridades públicas a estos datos. Dicha normativa permite a la Policía Judicial, en caso de concederse la autorización judicial solicitada sobre la base de esta, exigir a los proveedores de servicios de comunicaciones electrónicas que pongan a su disposición datos personales y que, de este modo, lleven a cabo, habida cuenta de la definición que figura en el artículo 2, letra b), de la Directiva 95/46, aplicable en el contexto de la Directiva 2002/58 en virtud del

artículo 2, párrafo primero, de esta, un «tratamiento» de tales datos, en el sentido de esas dos Directivas. En consecuencia, la citada normativa regula las actividades de los proveedores de servicios de comunicaciones electrónicas y por lo tanto está incluida dentro del ámbito de aplicación de la Directiva 2002/58.

39 En estas condiciones, la circunstancia invocada por el Gobierno español, según la cual esa solicitud de acceso se ha presentado en un procedimiento de instrucción penal, no hace que la Directiva 2002/58 sea inaplicable al litigio principal, de conformidad con su artículo 1, apartado 3.

40 También es irrelevante a estos efectos que la solicitud de acceso controvertida en el litigio principal tenga por objeto, tal y como se desprende de la respuesta escrita del Gobierno español a una pregunta formulada por el Tribunal de Justicia y como confirmaron tanto dicho Gobierno como el Ministerio Fiscal en la vista, permitir el acceso únicamente a los números de teléfono correspondientes a las tarjetas SIM activadas con el código IMEI del teléfono móvil sustraído y a los datos personales o de filiación de los titulares de estas tarjetas, como su nombre, apellidos y, en su caso, dirección, con exclusión de los datos relativos a las comunicaciones realizadas con esas tarjetas SIM y los datos de localización relativos al teléfono móvil sustraído.

41 En efecto, como ha señalado el Abogado General en el punto 54 de sus conclusiones, la Directiva 2002/58 regula, en virtud de sus artículos 1, apartado 1, y 3, todo tratamiento de datos personales en el marco de la prestación de servicios de comunicaciones electrónicas. Además, con arreglo al artículo 2, párrafo segundo, letra b), de dicha Directiva el concepto de «datos de tráfico» incluye «cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de la facturación de la misma».

42 A este respecto, tratándose más concretamente de datos personales o de filiación de los titulares de tarjetas SIM, del considerando 15 de la Directiva 2002/58 resulta que los datos de tráfico pueden incluir, en particular, el nombre y la dirección de la persona que emite una comunicación o que utiliza una conexión para llevar a cabo la comunicación. Los datos personales o de filiación de los titulares de tarjetas SIM pueden además resultar necesarios para la facturación de los servicios de comunicaciones electrónicas prestados y forman parte, por tanto, de los datos de tráfico, tal como se definen en el artículo 2, párrafo segundo, letra b), de dicha Directiva. En consecuencia, estos datos están incluidos en el ámbito de aplicación de la Directiva 2002/58.

43 Por consiguiente, el Tribunal de Justicia es competente para responder a la petición de decisión prejudicial planteada por el tribunal remitente.

Sobre la admisibilidad

44 El Gobierno español alega que la petición de decisión prejudicial es inadmisible porque no identifica con claridad las disposiciones del Derecho de la Unión sobre las que el Tribunal de Justicia debe pronunciarse. Además, la solicitud de la Policía Judicial controvertida en el litigio principal no versa sobre la interceptación de las comunicaciones realizadas a través de las tarjetas SIM activadas con el número IMEI del teléfono móvil sustraído, sino sobre una relación de tarjetas SIM y una relación de sus titulares, de modo que la confidencialidad de las comunicaciones no se vería afectada. Por tanto, en su opinión, el artículo 7 de la Carta, mencionado por las cuestiones prejudiciales, carece de pertinencia en el contexto del presente asunto.

45 Con arreglo a reiterada jurisprudencia del Tribunal de Justicia, en principio corresponde exclusivamente al juez nacional, que conoce del litigio y que debe asumir la responsabilidad de la decisión jurisdiccional que debe adoptarse, apreciar, a la luz de las particularidades de cada asunto, tanto la necesidad de una decisión prejudicial para poder dictar su sentencia como la pertinencia de las cuestiones que plantea al Tribunal de Justicia. Por consiguiente, cuando las cuestiones planteadas se refieren a la interpretación del Derecho de la Unión, el Tribunal de Justicia está, en principio, obligado a pronunciarse. La negativa del Tribunal de Justicia a pronunciarse sobre una cuestión prejudicial planteada por un órgano jurisdiccional nacional solo es posible cuando resulte evidente que la interpretación del Derecho de la Unión solicitada no tiene relación alguna con la realidad o con el objeto del litigio principal, cuando el problema sea de naturaleza hipotética o cuando el Tribunal de Justicia no disponga de los elementos de hecho y de Derecho necesarios para responder adecuadamente

a las cuestiones que se le hayan planteado (sentencia de 10 de julio de 2018, Jehovan Todistajat, C−25/17, EU:C:2018:551, apartado 31 y jurisprudencia citada).

46 En el presente asunto, el auto de remisión contiene los elementos de hecho y de Derecho suficientes tanto para la identificación de las disposiciones del Derecho de la Unión mencionadas en las cuestiones prejudiciales como para entender el alcance de estas cuestiones. En particular, del auto de remisión se desprende que las cuestiones prejudiciales planteadas tienen por objeto permitir al tribunal remitente apreciar si la norma nacional en la que se basa la solicitud de la Policía Judicial controvertida en el litigio principal persigue un objetivo que puede justificar una injerencia en los derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta, y en qué medida. Pues bien, según ese mismo tribunal, dicha norma nacional está comprendida en el ámbito de aplicación de la Directiva 2002/58, de modo que la Carta resulta aplicable en el litigio principal. Así, las cuestiones prejudiciales guardan una relación directa con el objeto del litigio principal y, por tanto, no pueden considerarse hipotéticas.

47 En estas circunstancias, las cuestiones prejudiciales son admisibles.

Sobre el fondo

48 Mediante sus dos cuestiones prejudiciales, que procede examinar conjuntamente, el tribunal remitente pregunta, en esencia, si el artículo 15, apartado 1, de la Directiva 2002/58, interpretado a la luz de los artículos 7 y 8 de la Carta, debe interpretarse en el sentido de que el acceso de las autoridades públicas 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 estos, consagrados en dichos artículos de la Carta, que presenta tal gravedad que el mencionado acceso debe limitarse, en el ámbito de la prevención, investigación, descubrimiento y persecución de delitos, a la lucha contra la delincuencia grave y, en caso afirmativo, con arreglo a qué criterios debe determinarse la gravedad del delito de que se trate.

49 A este respecto, del auto de remisión se desprende que, como ha señalado, en esencia, el Abogado General en el punto 38 de sus conclusiones, la petición de decisión prejudicial no tiene por objeto determinar si los datos personales de que se trata en el litigio principal han sido conservados por los proveedores de servicios de comunicaciones electrónicas de conformidad con los requisitos establecidos en el artículo 15, apartado 1, de la Directiva 2002/58, interpretado a la luz de los artículos 7 y 8 de la Carta. La petición tiene por objeto únicamente, como se desprende del apartado 46 de la presente sentencia, si el objetivo perseguido por la normativa controvertida en el litigio principal puede justificar el acceso de autoridades públicas, como la Policía Judicial, a dichos datos, y en qué medida, sin que los demás requisitos del acceso resultantes del citado artículo 15, apartado 1, sean objeto de dicha petición.

50 En particular, el tribunal remitente se pregunta qué elementos es preciso tener en cuenta para apreciar si los delitos respecto de los cuales puede autorizarse a las autoridades policiales, a efectos de investigación de un delito, a acceder a datos personales conservados por los proveedores de servicios de comunicaciones electrónicas son de una gravedad suficiente para justificar la injerencia que supone tal acceso en los derechos fundamentales garantizados en los artículos 7 y 8 de la Carta, tal como los interpreta el Tribunal de Justicia en sus sentencias de 8 de abril de 2014, Digital Rights Ireland y otros (C−293/12 y C−594/12, EU:C:2014:238), y Tele2 Sverige y Watson y otros.

51 En cuanto a la existencia de una injerencia en los derechos fundamentales, procede recordar que, como señaló el Abogado General en los puntos 76 y 77 de sus conclusiones, el acceso de las autoridades públicas a estos datos constituye 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. Tal acceso también constituye una injerencia en el derecho fundamental a la protección de los datos personales garantizado por el artículo 8 de la Carta, puesto que constituye un tratamiento de datos personales [véase, en este sentido, el dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartados 124 y 126 y jurisprudencia citada].

52 Por lo que respecta a los objetivos que pueden justificar una norma nacional, como la controvertida en el litigio principal, que regula el acceso de las autoridades públicas a los datos conservados por los proveedores de servicios de comunicaciones electrónicas y, por tanto, establece una excepción al principio de confidencialidad de las comunicaciones electrónicas, cabe recordar que la enumeración de los objetivos que figuran en el artículo 15, apartado 1, primera frase, de la Directiva 2002/58 tiene carácter exhaustivo, de modo que dicho acceso ha de responder efectiva y estrictamente a uno de ellos (véase, en este sentido, la sentencia Tele2 Sverige y Watson y otros, apartados 90 y 115).

53 Pues bien, por lo que se refiere al objetivo de la prevención, investigación, descubrimiento y persecución de delitos, procede observar que el tenor del artículo 15, apartado 1, primera frase, de la Directiva 2002/58 no limita este objetivo a la lucha contra los delitos graves, sino que se refiere a los «delitos» en general.

54 A este respecto, es cierto que el Tribunal de Justicia ha declarado que, en materia de prevención, investigación, descubrimiento y persecución de delitos, solo la lucha contra la delincuencia grave puede justificar un acceso a datos personales conservados por los proveedores de servicios de comunicaciones electrónicas que, considerados en su conjunto, permiten extraer conclusiones precisas sobre la vida privada de las personas cuyos datos han sido conservados (véase, en este sentido, la sentencia Tele2 Sverige y Watson y otros, apartado 99).

55 No obstante, el Tribunal de Justicia ha motivado esa interpretación basándose en 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 que supone la operación (véase, en este sentido, la sentencia Tele2 Sverige y Watson y otros, apartado 115).

56 En efecto, conforme al principio de proporcionalidad, en el ámbito de la prevención, investigación, descubrimiento y persecución de delitos solo puede justificar una injerencia grave el objetivo de luchar contra la delincuencia que a su vez esté también calificada de «grave».

57 En cambio, 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.

58 Así pues, ante todo, debe determinarse si, en el presente asunto, en función de las circunstancias del caso de autos, la injerencia en los derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta que entraña el acceso de la Policía Judicial a los datos de que se trata en el litigio principal debe considerarse «grave».

59 A este respecto, el oficio controvertido en el litigio principal, por el que la Policía Judicial solicita, a efectos de la investigación de un delito, autorización judicial para acceder a los datos personales conservados por los proveedores de servicios de comunicaciones electrónicas, tiene por único objeto identificar a los titulares de las tarjetas SIM activadas durante un período de doce días con el número IMEI del teléfono móvil sustraído. De este modo, como se ha señalado en el apartado 40 de la presente sentencia, esta solicitud no tiene más objeto que el acceso a los números de teléfono correspondientes a las tarjetas SIM así como a los datos personales o de filiación de los titulares de dichas tarjetas, como su nombre, apellidos y, en su caso, la dirección. En cambio, esos datos no se refieren, como confirmaron tanto el Gobierno español como el Ministerio Fiscal en la vista, a las comunicaciones efectuadas con el teléfono móvil sustraído ni a la localización de este.

60 Por tanto, los datos a que se refiere la solicitud de acceso controvertida en el litigio principal solo permiten vincular, durante un período determinado, 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. Sin un cotejo con los datos relativos a las comunicaciones realizadas con esas tarjetas SIM y de localización, estos datos no permiten conocer la fecha, la hora, la duración o los destinatarios de las comunicaciones efectuadas con las tarjetas SIM en cuestión, ni los lugares en que estas comunicaciones tuvieron lugar, ni la frecuencia de estas con determinadas personas durante un período concreto. Por tanto, dichos datos no permiten extraer conclusiones precisas sobre la vida privada de las personas cuyos datos se ven afectados.

61 En tales circunstancias, el acceso limitado únicamente a los datos cubiertos por la solicitud controvertida en el litigio principal no puede calificarse de injerencia «grave» en los derechos fundamentales de los individuos cuyos datos se ven afectados.

62 En consecuencia, como se desprende de los apartados 53 a 57 de la presente sentencia, la injerencia que supone el acceso a dichos datos puede estar justificada por el objetivo de prevenir, investigar, descubrir y perseguir «delitos» en general, al que se refiere el artículo 15, apartado 1, primera frase, de la Directiva 2002/58, sin que sea necesario que dichos delitos estén calificados como «graves».

63 Habida cuenta de las consideraciones anteriores, procede responder a las cuestiones prejudiciales planteadas que el artículo 15, apartado 1, de la Directiva 2002/58, a la luz de los artículos 7 y 8 de la Carta, debe interpretarse en el sentido de que el acceso de las autoridades públicas 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 estos, consagrados en los citados artículos de la Carta, que no presenta una gravedad tal que dicho acceso deba limitarse, en el ámbito de la prevención, investigación, descubrimiento y persecución de delitos, a la lucha contra la delincuencia grave.

Costas

64 Dado que el procedimiento tiene, para las partes del litigio principal, el carácter de un incidente promovido ante el órgano jurisdiccional remitente, corresponde a este resolver sobre las costas. Los gastos efectuados por quienes, no siendo partes del litigio principal, han presentado observaciones ante el Tribunal de Justicia no pueden ser objeto de reembolso.

En virtud de todo lo expuesto, el Tribunal de Justicia (Gran Sala) declara:

El artículo 15, apartado 1, de la 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), en su versión modificada por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, a la luz de los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea, debe interpretarse en el sentido de que el acceso de las autoridades públicas 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 estos, consagrados en los citados artículos de la Carta de los Derechos

Fundamentales, que no presenta una gravedad tal que dicho acceso deba limitarse, en el ámbito de la prevención, investigación, descubrimiento y persecución de delitos, a la lucha contra la delincuencia grave.

Lenaerts	Tizzano	Silva de Lapuerta
von Danwitz	Da Cruz Vilaça	Fernlund
Vajda	Juhász	Borg Barthet
Toader	Safjan	Šváby

Berger Jarašiūnas Regan

Pronunciada en audiencia pública en Luxemburgo, a 2 de octubre de 2018.

El Secretario El Presidente

A. Calot Escobar K. Lenaerts

---

* Lengua de procedimiento: español.