SENTENCIA DEL TRIBUNAL DE JUSTICIA (Sala Primera)

de 7 de septiembre de 2023 (*)

«Procedimiento prejudicial — Telecomunicaciones — Tratamiento de los datos personales en el sector de las comunicaciones electrónicas — Directiva 2002/58/CE — Ámbito de aplicación — Artículo 15, apartado 1 — Datos conservados por los proveedores de servicios de comunicaciones electrónicas y puestos a disposición de las autoridades encargadas de los procesos penales — Utilización posterior de esos datos con ocasión de una investigación sobre una conducta indebida en el ejercicio del cargo»

En el asunto C-162/22,

que tiene por objeto una petición de decisión prejudicial planteada, con arreglo al artículo 267 TFUE, por el Lietuvos vyriausiasis administracinis teismas (Tribunal Supremo de lo Contencioso-Administrativo de Lituania), mediante resolución de 24 de febrero de 2022, recibida en el Tribunal de Justicia el 3 de marzo de 2022, en el procedimiento incoado por

A. G.

con intervención de:

Lietuvos Respublikos generalinė prokuratūra,

EL TRIBUNAL DE JUSTICIA (Sala Primera),

integrado por el Sr. A. Arabadjiev, Presidente de Sala, y los Sres. P. G. Xuereb (Ponente), T. von Danwitz y A. Kumin y la Sra. I. Ziemele, Jueces;

Abogado General: Sr. M. Campos Sánchez-Bordona;

Secretaria: Sra. A. Lamote, administradora;

habiendo considerado los escritos obrantes en autos y celebrada la vista el 2 de febrero de 2023;

consideradas las observaciones presentadas:

– en nombre de A. G., por el Sr. G. Danėlius, advokatas;

– en nombre del Gobierno lituano, por el Sr. S. Grigonis y las Sras. V. Kazlauskaitė-Švenčionienė y V. Vasiliauskienė, en calidad de agentes;

– en nombre del Gobierno checo, por los Sres. O. Serdula, M. Smolek y J. Vláčil, en calidad de agentes;

– en nombre del Gobierno estonio, por la Sra. M. Kriisa, en calidad de agente;

– en nombre de Irlanda, por la Sra. M. Browne y los Sres. A. Joyce y M. Tierney, en calidad de agentes, asistidos por el Sr. D. Fennelly, BL;

– en nombre del Gobierno francés, por el Sr. R. Bénard, en calidad de agente;

– en nombre del Gobierno italiano, por la Sra. G. Palmieri, en calidad de agente, asistida por el Sr. A. Grumetto, avvocato dello Stato;

– en nombre del Gobierno húngaro, por la Sra. Zs. Biró-Tóth y el Sr. M. Z. Fehér, en calidad de agentes;

– en nombre de la Comisión Europea, por los Sres. S. L. Kalėda, H. Kranenborg, P.-J. Loewenthal y F. Wilman, en calidad de agentes;

oídas las conclusiones del Abogado General, presentadas en audiencia pública el 30 de marzo de 2023;

dicta la siguiente

Sentencia

1 La petición de decisión prejudicial tiene por objeto 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»).

2 Esta petición se ha presentado en el contexto de un procedimiento incoado por A. G. en relación con la legalidad de determinadas resoluciones de la Lietuvos Respublikos generalinė prokuratūra (Fiscalía General de la República de Lituania; en lo sucesivo, «Fiscalía General») por las que se le suspendió de sus funciones de fiscal.

Marco jurídico

Derecho de la Unión

3 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.

[…]

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.»

4 El artículo 5 de dicha Directiva, titulado «Confidencialidad de las comunicaciones», establece, en su apartado 1, lo siguiente:

«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. El presente apartado no impedirá el almacenamiento técnico necesario para la conducción de una comunicación, sin perjuicio del principio de confidencialidad.»

5 El artículo 15 de la mencionada Directiva, titulado «Aplicación de determinadas disposiciones de la Directiva 95/46/CE», dispone 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/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)]. 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 [TUE].»

Derecho lituano

Ley de Comunicaciones Electrónicas

6 El artículo 65, apartado 2, de la Lietuvos Respublikos elektroninių ryšių įstatymas (Ley de la República de Lituania de Comunicaciones Electrónicas), de 15 de abril de 2004 (Žin., 2004, n.º 69-2382), en su versión aplicable a los hechos del litigio principal (en lo sucesivo, «Ley de Comunicaciones Electrónicas»), obliga a los proveedores de servicios de comunicaciones electrónicas a conservar los datos mencionados en el anexo 1 de dicha Ley y, en su caso, a ponerlos a disposición de las autoridades competentes con el fin de que estas puedan utilizarlos en la lucha contra la delincuencia grave.

7 De conformidad con el anexo 1 de la Ley de Comunicaciones Electrónicas, las categorías de datos que deben conservarse son las siguientes:

«1. Los datos necesarios para rastrear y determinar el origen de una comunicación: […] 2. Los datos necesarios para determinar el destino de una comunicación: […] 3. Los datos necesarios para determinar la fecha, hora y duración de una comunicación: […] 4. Los datos necesarios para determinar el tipo de comunicación: […] 5. Los datos necesarios para determinar el dispositivo de comunicación de los usuarios o lo que podría ser su dispositivo de comunicación: […] 6. Los datos necesarios para localizar el dispositivo de comunicación móvil: […]».

8 De conformidad con el artículo 77, apartado 4, de dicha Ley, cuando exista una resolución judicial motivada u otra base jurídica prevista por la ley, los proveedores de servicios de comunicaciones electrónicas deberán hacer técnicamente posible, en particular para los órganos de investigación criminal y los órganos de instrucción, según las modalidades previstas por la Lietuvos Respublikos baudžiamojo proceso kodeksas (Ley de Enjuiciamiento Criminal de la República de Lituania; en lo sucesivo «Ley de Enjuiciamiento Criminal»), el control del contenido de las comunicaciones realizadas a través de las redes de comunicaciones electrónicas.

Ley de Inteligencia Criminal

9 El artículo 6, apartado 3, punto 1, de la Lietuvos Respublikos kriminalinės žvalgybos Istatymas (Ley de la República de Lituania de Inteligencia Criminal), de 2 de octubre de 2012 (Žin., 2012, n.º 122-6093), en su versión aplicable a los hechos del litigio principal (en lo sucesivo, «Ley de Inteligencia Criminal»), dispone que, cuando se cumplan las condiciones previstas por dicha Ley para justificar una operación de investigación criminal, y previa autorización del Ministerio Fiscal o de un órgano jurisdiccional, los órganos de investigación criminal podrán, además de lo enumerado en los apartados 1 y 2 del mismo artículo, recabar información de los proveedores de servicios de comunicaciones electrónicas.

10 El artículo 8, apartado 1, de dicha Ley establece que los organismos de investigación en materia penal llevarán a cabo una investigación, en particular, cuando se disponga de información sobre la preparación o la comisión de una infracción muy grave, grave o relativamente grave, o sobre las personas que preparan, comenten o hubieren cometido tal infracción. El artículo 8, apartado 3, de la citada Ley precisa que, si tal investigación pone de manifiesto la existencia de indicios de delito, se iniciará de inmediato una instrucción penal.

11 A tenor del artículo 19, apartado 1, punto 5, de la Ley de Inteligencia Criminal, la información procedente de operaciones de investigación criminal podrá ser utilizada en los casos establecidos en los apartados 3 y 4 del mismo artículo y en otros supuestos previstos por la ley. En virtud del apartado 3 de dicho artículo, la información procedente de operaciones de investigación criminal relativa a un hecho que presente las características de una infracción relacionada con la corrupción podrá ser desclasificada, previo acuerdo del Ministerio Fiscal, y utilizada en el marco de una investigación sobre faltas disciplinarias o en el ejercicio del cargo.

Ley de Enjuiciamiento Criminal

12 El artículo 154 de la Ley de Enjuiciamiento Criminal establece que, previa resolución de un juez de instrucción dictada a petición de un miembro del Ministerio Fiscal, un investigador podrá escuchar y transcribir las conversaciones realizadas a través de las redes de comunicaciones electrónicas y controlar, grabar y conservar otras informaciones conducidas a través de las redes de comunicaciones electrónicas, en particular, si existen razones para pensar que ello permitirá obtener datos sobre una infracción muy grave o grave en fase de preparación o de comisión o que se hubiere cometido, o sobre una infracción relativamente grave o no grave.

13 El artículo 177, apartado 1, de dicha Ley dispone que los datos de la instrucción son confidenciales y que, hasta el examen judicial del asunto, solo podrán divulgarse mediando autorización del Ministerio Fiscal y únicamente en la medida en que se considere justificado.

14 A efectos de la aplicación del artículo 177 de dicha Ley, son aplicables las Ikiteisminio tyrimo duomenų teikimo ir panaudojimo ne baudžiamojo persekiojimo tikslais ir ikiteisminio tyrimo duomenų apsaugos rekomendacijos (Recomendaciones sobre la puesta a disposición y la utilización de los datos de la investigación preliminar con fines ajenos a la instrucción y la protección de los datos de la investigación preliminar), aprobadas por el Decreto n.º I-279 del fiscal general de 17 de agosto de 2017 (TAR, 2017, n.º 2017-13413), en su versión modificada, por última vez, por el Decreto n.º I-211, de 25 de junio de 2018.

15 El punto 23 de dichas recomendaciones establece que, cuando el fiscal reciba una solicitud de acceso a datos procedentes de la instrucción, este decidirá si procede facilitarlos. Si se adopta la decisión de facilitarlos, el fiscal especificará en qué medida podrán facilitarse los datos a que se refiere la solicitud.

Litigio principal y cuestión prejudicial

16 La Fiscalía General incoó una investigación administrativa contra el demandante en el litigio principal, que en esa época ejercía las funciones de fiscal en una fiscalía lituana, por existir indicios de que este había proporcionado ilegalmente al sospechoso y a su abogado, en el marco de una instrucción que dirigía, información relevante de dicha instrucción.

17 En su informe sobre dicha investigación, la comisión de la Fiscalía General declaró que el demandante en el litigio principal había incurrido efectivamente en una conducta indebida en el ejercicio de su cargo.

18 Según el citado informe, dicha conducta indebida quedaba demostrada por los datos recabados durante la investigación administrativa. En concreto, la información obtenida durante las operaciones de investigación criminal y los datos recabados en las dos instrucciones penales confirmaban la existencia de comunicaciones telefónicas entre el demandante en el litigio principal y el abogado del sospechoso durante la instrucción que el demandante dirigía contra este último. El mencionado informe señalaba, además, que un auto judicial había autorizado la interceptación y la grabación de la información transmitida a través de las redes de comunicaciones electrónicas relativa al abogado en cuestión y que otro auto judicial había autorizado la misma medida respecto del demandante en el litigio principal.

19 Sobre la base del mismo informe, la Fiscalía General adoptó dos resoluciones mediante las cuales, por un lado, impuso al demandante en el litigio principal una sanción consistente en la revocación de sus funciones y, por otro lado, le separó del servicio.

20 El demandante en el litigio principal interpuso un recurso ante el Vilniaus apygardos administracinis teismas (Tribunal Regional de lo Contencioso-Administrativo de Vilna, Lituania) solicitando, en particular, la anulación de ambas resoluciones.

21 Mediante sentencia de 16 de julio de 2021, dicho órgano jurisdiccional desestimó el recurso del demandante en el litigio principal al considerar, en particular, que las operaciones de investigación criminal efectuadas en dicho asunto eran conformes a Derecho y que la información recabada de conformidad con las disposiciones de la Ley de Inteligencia Criminal había sido utilizada legalmente para apreciar la existencia de una conducta indebida supuestamente cometida por el demandante en el litigio principal en el ejercicio de su cargo.

22 El demandante en el litigio principal interpuso recurso de apelación ante el Lietuvos vyriausiasis administracinis teismas (Tribunal Supremo de lo Contencioso-Administrativo de Lituania), el órgano jurisdiccional remitente, alegando que el acceso por parte de los órganos de investigación, en el marco de una operación de investigación criminal, a los datos de tráfico y al contenido mismo de las comunicaciones electrónicas constituía una vulneración de los derechos fundamentales de tal gravedad que, habida cuenta de las disposiciones de la Directiva 2002/58 y de la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, «Carta»), dicho acceso solo podía concederse a los efectos de la lucha contra las infracciones graves. Pues bien, según el demandante, el artículo 19, apartado 3, de la Ley de Inteligencia Criminal establece que tales datos pueden utilizarse para investigar no solo infracciones graves, sino también faltas disciplinarias o faltas cometidas en el ejercicio del cargo relacionadas con actos de corrupción.

23 Según el órgano jurisdiccional remitente, las cuestiones prejudiciales planteadas por el demandante en el litigio principal se refieren a dos elementos, a saber, por un lado, el acceso a los datos conservados por los proveedores de servicios de comunicaciones electrónicas con fines distintos de la lucha contra las infracciones graves y la prevención de las amenazas graves contra la seguridad pública y, por otro lado, una vez obtenido dicho acceso, la utilización de esos datos para investigar conductas indebidas en el ejercicio del cargo relacionadas con la corrupción.

24 Dicho órgano jurisdiccional recuerda que de la jurisprudencia del Tribunal de Justicia, en particular de la sentencia de 6 de octubre de 2020, Privacy International (C-623/17, EU:C:2020:790), apartado 39, se desprende, por un lado, que el artículo 15, apartado 1, de la Directiva 2002/58, en relación con el artículo 3 de esta, 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 de localización, sino también una medida legislativa que les obliga a permitir a las autoridades nacionales competentes el acceso a estos datos. Por otro lado, el órgano jurisdiccional remitente afirma que de esta jurisprudencia, en particular de la sentencia de 2 de marzo de 2021, Prokuratuur (Condiciones de acceso a los datos relativos a las comunicaciones electrónicas) (C-746/18, EU:C:2021:152), apartados 33 y 35, se desprende que, en lo que atañe al objetivo de prevención, investigación, descubrimiento y persecución de delitos, de conformidad con el principio de proporcionalidad, solo la lucha contra la delincuencia grave y la prevención de las amenazas graves contra la seguridad pública pueden justificar las injerencias graves en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta, como las que supone la conservación de los datos de tráfico y de los datos de localización, sea dicha conservación generalizada e indiferenciada o selectiva.

25 Sin embargo, según señala el mencionado órgano jurisdiccional, el Tribunal de Justicia aún no se ha pronunciado sobre la incidencia de la utilización posterior de los datos de que trata en los derechos fundamentales. En estas circunstancias, el órgano jurisdiccional remitente se pregunta si dicha utilización posterior debe asimismo considerarse constitutiva de una injerencia en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta de tal gravedad que solo la lucha contra la delincuencia grave y la prevención de las amenazas graves contra la seguridad pública pueden justificarla, lo que excluiría la posibilidad de utilizar esos datos en investigaciones relativas a conductas indebidas en el ejercicio del cargo relacionadas con la corrupción.

26 En estas circunstancias, el Lietuvos vyriausiasis administracinis teismas (Tribunal Supremo de lo Contencioso-Administrativo de Lituania) decidió suspender el procedimiento y plantear al Tribunal de Justicia la siguiente cuestión prejudicial:

«¿Debe interpretarse el artículo 15, apartado 1, de la Directiva [2002/58], analizado en relación con los artículos 7, 8, 11 y 52, apartado 1, de la [Carta], en el sentido de que prohíbe a las autoridades públicas competentes utilizar datos conservados por proveedores de servicios de comunicaciones electrónicas que puedan proporcionar información sobre los datos de un usuario de un medio de comunicaciones electrónicas, y las comunicaciones realizadas por ese usuario, en el marco de investigaciones de conductas indebidas relacionadas con la corrupción en el ejercicio del cargo, con independencia de que el acceso a esos datos se haya concedido, en el caso concreto, con el

fin de luchar contra la delincuencia grave y prevenir las amenazas graves contra la seguridad pública?»

Sobre la cuestión prejudicial

27 Mediante su cuestión prejudicial, el órgano jurisdiccional remitente pregunta, en esencia, si el artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta, debe interpretarse en el sentido de que se opone a que datos personales relativos a comunicaciones electrónicas que hayan sido conservados, en aplicación de una medida legislativa adoptada en virtud de dicha disposición, por los proveedores de servicios de comunicaciones electrónicas y que posteriormente, en aplicación de dicha medida, se hayan puesto a disposición de las autoridades competentes a efectos de la lucha contra la delincuencia grave, puedan utilizarse en el marco de investigaciones relativas a conductas indebidas en el ejercicio del cargo relacionadas con la corrupción.

28 Con carácter preliminar, es preciso señalar que de la resolución de remisión se desprende que si bien el expediente administrativo relativo al procedimiento que dio lugar a las resoluciones controvertidas en el litigio principal, a que hace referencia el apartado 19 de la presente sentencia, incluía también información que había sido recabada por las autoridades competentes mediante la interceptación y la grabación de comunicaciones electrónicas que habían sido autorizadas, a los efectos del ejercicio de acciones penales, por dos resoluciones judiciales, no es menos cierto que el órgano jurisdiccional remitente no se pregunta sobre la utilización de datos personales recabados sin la intervención de los proveedores de servicios de comunicaciones electrónicas, sino sobre la utilización posterior de los datos personales conservados por tales proveedores en virtud de una medida legislativa del Estado miembro que les impone tal obligación de conservación, en virtud del artículo 15, apartado 1, de la Directiva 2002/58.

29 A este respecto, de las indicaciones que figuran en la petición de decisión prejudicial se desprende que los datos a que se refiere la cuestión planteada son los conservados en virtud del artículo 65, apartado 2, de la Ley de Comunicaciones Electrónicas, en relación con el anexo 1 de dicha Ley, que impone a los proveedores de servicios de comunicaciones electrónicas la obligación de conservar, de manera generalizada e indiferenciada, los datos de tráfico y de localización relativos a tales comunicaciones a efectos de la lucha contra la delincuencia grave.

30 Por lo que respecta a las condiciones en las que esos datos pueden utilizarse en el marco de procedimientos administrativos relativos a conductas indebidas en el ejercicio del cargo relacionadas con la corrupción, conviene recordar, antes de nada, que el acceso a dichos datos solo puede concederse, en aplicación de una medida adoptada al amparo del artículo 15, apartado 1, de la Directiva 2002/58, para el caso de que esos datos hayan sido conservados por tales proveedores de conformidad con dicha disposición [véase, en este sentido, la sentencia de 2 de marzo de 2021, Prokuratuur (Condiciones de acceso a los datos relativos a las comunicaciones electrónicas), C-746/18, EU:C:2021:152, apartado 29 y jurisprudencia citada]. Además, la utilización posterior de los datos de tráfico y de localización relativos a tales comunicaciones a efectos de la lucha contra la delincuencia grave solo es posible si, por un lado, la conservación de dichos datos por los proveedores de servicios de comunicaciones electrónicas era conforme con el artículo 15, apartado 1, de la Directiva 2002/58, tal como lo interpreta la jurisprudencia del Tribunal de Justicia, y si, por otro lado, el acceso a los mencionados datos concedido a las autoridades competentes también era conforme con dicha disposición.

31 A este respecto, el Tribunal de Justicia ya ha declarado que el artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta, se opone a medidas legislativas nacionales que establezcan, con carácter preventivo, a efectos de la lucha contra la delincuencia grave y la prevención de amenazas graves contra la seguridad pública, una conservación generalizada e indiferenciada de los datos de tráfico y de localización (sentencia de 20 de septiembre de 2022, SpaceNet y Telekom Deutschland, C-793/19 y C-794/19, EU:C:2022:702, apartados 74 y 131 y jurisprudencia citada). En cambio, el Tribunal de Justicia ha precisado que dicho artículo 15, apartado 1, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta, no se opone a medidas legislativas que permitan, a efectos de la lucha contra la delincuencia grave y de la prevención de amenazas graves contra la seguridad pública,

– una conservación selectiva de los datos de tráfico y de localización que esté delimitada, sobre la base de elementos objetivos y no discriminatorios, en función de las categorías de personas afectadas o mediante un criterio geográfico, para un período temporalmente limitado a lo estrictamente necesario, pero que podrá renovarse;

– una conservación generalizada e indiferenciada de las direcciones IP atribuidas al origen de una conexión, para un período temporalmente limitado a lo estrictamente necesario;

– una conservación generalizada e indiferenciada de los datos relativos a la identidad civil de los usuarios de medios de comunicaciones electrónicas, y

– el recurso a un requerimiento efectuado a los proveedores de servicios de comunicaciones electrónicas, mediante una decisión de la autoridad competente sujeta a un control jurisdiccional efectivo, para que procedan, durante un período determinado, a la conservación rápida de los datos de tráfico y de localización de que dispongan estos proveedores de servicios,

siempre que dichas medidas garanticen, mediante normas claras y precisas, que la conservación de los datos en cuestión está supeditada al respeto de las condiciones materiales y procesales correspondientes y que las personas afectadas disponen de garantías efectivas contra los riesgos de abuso (sentencia de 20 de septiembre de 2022, SpaceNet y Telekom Deutschland, C-793/19 y C-794/19, EU:C:2022:702, apartado 75 y jurisprudencia citada).

32 Por lo que respecta a los objetivos que pueden justificar la utilización, por las autoridades públicas, de datos conservados por los proveedores de servicios de comunicaciones electrónicas en aplicación de una medida conforme con esas disposiciones, procede recordar que el artículo 15, apartado 1, de la Directiva 2002/58 permite a los Estados miembros establecer excepciones a la obligación de principio, enunciada en el artículo 5, apartado 1, de dicha Directiva, de garantizar la confidencialidad de los datos personales y a las obligaciones correspondientes, mencionadas en particular en los artículos 6 y 9 de dicha Directiva, 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 para la prevención, investigación, descubrimiento y persecución de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas. 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 uno de esos motivos (sentencia de 6 de octubre de 2020, La Quadrature du Net y otros, C-511/18, C-512/18 y C-520/18, EU:C:2020:791, apartado 110).

33 En consecuencia, el artículo 15, apartado 1, de la Directiva 2002/58 no puede justificar que la excepción a la obligación de principio de garantizar la confidencialidad de las comunicaciones electrónicas y de los datos relativos a ellas y, en particular, a la prohibición de almacenar esos datos, prevista en el artículo 5 de la citada Directiva, se convierta en la regla si no se quiere privar en gran medida a esta última disposición de su alcance (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 40).

34 Por lo que respecta a los objetivos que pueden justificar una limitación de los derechos y de las obligaciones previstos, en particular, en los artículos 5, 6 y 9 de la Directiva 2002/58, el Tribunal de Justicia ya ha declarado que la enumeración de los objetivos que figuran en el artículo 15, apartado 1, primera frase, de dicha Directiva tiene carácter exhaustivo, de modo que la medida legal que se adopte en virtud de esta disposición ha de responder efectiva y estrictamente a uno de ellos (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 41).

35 Por lo que toca a los objetivos de interés general que permiten justificar una medida adoptada en virtud del artículo 15, apartado 1, de la Directiva 2002/58, de la jurisprudencia del Tribunal de Justicia se desprende que, conforme al principio de proporcionalidad, existe una jerarquía entre dichos objetivos en función de su importancia respectiva y que la importancia del objetivo perseguido por tal medida debe ser correlativa a la gravedad de la injerencia que supone la medida (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 56).

36 A este respecto, la importancia del objetivo de protección de la seguridad nacional, interpretado a la luz del artículo 4 TUE, apartado 2, según el cual la protección de la seguridad nacional sigue siendo responsabilidad exclusiva de cada Estado miembro, supera la de los demás objetivos contemplados en el artículo 15, apartado 1, de la Directiva 2002/58, en particular los objetivos de combatir la delincuencia en general, incluso grave, y de protección de la seguridad pública. Por lo tanto, sin perjuicio del cumplimiento de los demás requisitos establecidos en el artículo 52, apartado 1, de la Carta, el objetivo de protección de la seguridad nacional puede justificar medidas que supongan injerencias en los derechos fundamentales más graves que las que podrían justificar

esos otros objetivos (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 57 y jurisprudencia citada).

37 En lo que atañe al objetivo de prevención, investigación, descubrimiento y persecución de delitos, el Tribunal de Justicia ha señalado que, de conformidad con el principio de proporcionalidad, solo la lucha contra la delincuencia grave y la prevención de las amenazas graves contra la seguridad pública pueden justificar las injerencias graves en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta, como las que supone la conservación de los datos de tráfico y de los datos de localización. En consecuencia, solo las injerencias en tales derechos fundamentales que no presenten un carácter grave pueden estar justificadas por el objetivo de prevención, investigación, descubrimiento y persecución de delitos en general (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 59 y jurisprudencia citada).

38 De dicha jurisprudencia se desprende que si bien la lucha contra la delincuencia grave y la prevención de amenazas graves para la seguridad pública son de una importancia menor, en la jerarquía de los objetivos de interés general, que la protección de la seguridad nacional (véase, en este sentido, la sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 99), su importancia supera a la de la lucha contra la delincuencia en general y a la de la prevención de amenazas no graves contra la seguridad pública.

39 En este contexto, se debe no obstante recordar que, como también resulta del apartado 31 de la presente sentencia, la posibilidad de que los Estados miembros justifiquen una limitación de los derechos y obligaciones previstos, en particular, en los artículos 5, 6 y 9 de la Directiva 2002/58 debe apreciarse determinando la gravedad de la injerencia que supone esa limitación y comprobando que la importancia del objetivo de interés general perseguido por dicha limitación guarde relación con tal gravedad (sentencia de 6 de octubre de 2020, La Quadrature du Net y otros, C-511/18, C-512/18 y C-520/18, EU:C:2020:791, apartado 131).

40 Por otro lado, como ya ha declarado el Tribunal de Justicia, el acceso a los datos de tráfico y de localización conservados por los proveedores con arreglo a una medida adoptada de conformidad con el artículo 15, apartado 1, de la Directiva 2002/58, que debe efectuarse respetando los requisitos que se derivan de la jurisprudencia que ha interpretado la Directiva 2002/58, solo puede estar justificado, en principio, por el objetivo de interés general para el que dicha conservación se impuso a estos proveedores. Solo cabría una solución diferente si la importancia del objetivo perseguido por el acceso fuera mayor que la del objetivo que justificó la conservación (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 98 y jurisprudencia citada).

41 Pues bien, estas consideraciones se aplican *mutatis mutandis* a una utilización posterior de los datos de tráfico y de localización conservados por proveedores de servicios de comunicaciones electrónicas en aplicación de una medida adoptada en virtud del artículo 15, apartado 1, de la Directiva 2002/58 a efectos de la lucha contra la delincuencia grave. En efecto, tales datos no pueden, tras haber sido conservados y puestos a disposición de las autoridades competentes a efectos de la lucha contra la delincuencia grave, transmitirse a otras autoridades ni utilizarse para alcanzar objetivos como, en el presente asunto, la lucha contra las conductas indebidas en el ejercicio del cargo relacionadas con la corrupción, que son de una importancia menor, en la jerarquía de los objetivos de interés general, que el de la lucha contra la delincuencia grave y el de la prevención de las amenazas graves contra la seguridad pública. En efecto, autorizar, en tal situación, el acceso a los datos conservados sería contrario a la jerarquía de objetivos de interés general recordada en los apartados 33, 35 a 37 y 40 de la presente sentencia (véase, en este sentido, la sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 99).

42 Por lo que respecta a la alegación formulada por el Gobierno checo y por Irlanda en sus observaciones escritas, según la cual un procedimiento disciplinario relativo a conductas indebidas en el ejercicio del cargo relacionadas con la corrupción podría estar relacionado con la protección de la seguridad pública, basta con señalar que, en su resolución de remisión, el órgano jurisdiccional remitente no ha hecho referencia a ninguna amenaza grave para la seguridad pública.

43 Por otra parte, si bien es cierto que las investigaciones administrativas relativas a faltas disciplinarias o en el ejercicio del cargo relacionadas con actos de corrupción pueden desempeñar un papel importante en la lucha contra tales actos, una medida legislativa que prevea tales

investigaciones no responde ni efectiva ni estrictamente al objetivo de persecución y sanción de los delitos, establecido en el artículo 15, apartado 1, primera frase, de la Directiva 2002/58, que solo se refiere a procesos penales.

44 A la luz de lo anterior, procede responder a la cuestión prejudicial planteada que el artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta, debe interpretarse en el sentido de que se opone a que datos personales relativos a comunicaciones electrónicas que hayan sido conservados, en aplicación de una medida legislativa adoptada en virtud de dicha disposición, por los proveedores de servicios de comunicaciones electrónicas y que, posteriormente, en aplicación de dicha medida, se hayan puesto a disposición de las autoridades competentes a efectos de la lucha contra la delincuencia grave puedan utilizarse en el marco de investigaciones relativas a conductas indebidas en el ejercicio del cargo relacionadas con la corrupción.

Costas

45 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 (Sala Primera) 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, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea,

ha de interpretarse en el sentido de que

se opone a que datos personales relativos a comunicaciones electrónicas que hayan sido conservados, en aplicación de una medida legislativa adoptada en virtud de dicha disposición, por los proveedores de servicios de comunicaciones electrónicas y que, posteriormente, en aplicación de dicha medida, se hayan puesto a disposición de las autoridades competentes a efectos de la lucha contra la delincuencia grave puedan utilizarse en el marco de investigaciones relativas a conductas indebidas en el ejercicio del cargo relacionadas con la corrupción.

Firmas