Recopilación de la Jurisprudencia

SENTENCIA DEL TRIBUNAL DE JUSTICIA (Gran Sala)

de 2 de marzo de 2021*

«Procedimiento prejudicial — Tratamiento de los datos personales en el sector de las comunicaciones electrónicas — Directiva 2002/58/CE — Proveedores de servicios de comunicaciones electrónicas — Confidencialidad de las comunicaciones — Limitaciones — Artículo 15, apartado 1 — Artículos 7, 8, 11 y 52, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea — Normativa que establece la conservación generalizada e indiferenciada de los datos de tráfico y de localización por los proveedores de servicios de comunicaciones electrónicas — Acceso de las autoridades nacionales a los datos conservados con fines de investigación — Lucha contra la delincuencia en general — Autorización del Ministerio Fiscal — Utilización de los datos como pruebas en el proceso penal — Admisibilidad»

En el asunto C-746/18,

que tiene por objeto una petición de decisión prejudicial planteada, con arreglo al artículo 267 TFUE, por el Riigikohus (Tribunal Supremo, Estonia), mediante resolución de 12 de noviembre de 2018, recibida en el Tribunal de Justicia el 29 de noviembre de 2018, en el procedimiento penal contra

H. K.,

con intervención de:

Prokuratuur,

EL TRIBUNAL DE JUSTICIA (Gran Sala),

integrado por el Sr. K. Lenaerts, Presidente, la Sra. R. Silva de Lapuerta, Vicepresidenta, los Sres. J.-C. Bonichot y A. Arabadjiev, la Sra. A. Prechal y el Sr. L. Bay Larsen, Presidentes de Sala, y los Sres. T. von Danwitz (Ponente) y M. Safjan, la Sra. K. Jürimäe y los Sres. C. Lycourgos y P. G. Xuereb, Jueces;

Abogado General: Sr. G. Pitruzzella;

Secretaria: Sra. C. Strömholm, administradora;

habiendo considerado los escritos obrantes en autos y celebrada la vista el 15 de octubre de 2019;

consideradas las observaciones presentadas:

– en nombre de H. K., por el Sr. S. Reinsaar, vandeadvokaat;

– en nombre del Prokuratuur, por el Sr. T. Pern y la Sra. M. Voogma, en calidad de agentes;

* Lengua de procedimiento: estonio.

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

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

– en nombre de Irlanda, por las Sras. M. Browne, G. Hodge y J. Quaney y por el Sr. A. Joyce, en calidad de agentes, asistidos por el Sr. D. Fennelly, Barrister;

– en nombre del Gobierno francés, inicialmente por los Sres. D. Dubois y D. Colas y por las Sras. E. de Moustier y A.-L. Desjonquères, y posteriormente por el Sr. D. Dubois y las Sras. E. de Moustier y A.-L. Desjonquères, en calidad de agentes;

– en nombre del Gobierno letón, inicialmente por las Sras. V. Kalniņa e I. Kucina, y posteriormente por las Sras. V. Soņeca y V. Kalniņa, en calidad de agentes;

– en nombre del Gobierno húngaro, por el Sr. M. Z. Fehér y la Sra. A. Pokoraczki, en calidad de agentes;

– en nombre del Gobierno polaco, por el Sr. B. Majczyna, en calidad de agente;

– en nombre del Gobierno portugués, por el Sr. L. Inez Fernandes y las Sras. P. Barros da Costa, L. Medeiros e I. Oliveira, en calidad de agentes;

– en nombre del Gobierno finlandés, por el Sr. J. Heliskoski, en calidad de agente;

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

– en nombre de la Comisión Europea, inicialmente por los Sres. H. Kranenborg y M. Wasmeier y por las Sras. P. Costa de Oliveira y K. Toomus, y posteriormente por los Sres. H. Kranenborg y M. Wasmeier y por la Sra. E. Randvere, en calidad de agentes;

oídas las conclusiones del Abogado General, presentadas en audiencia pública el 21 de enero de 2020;

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»), en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, «Carta»).

2 Esta petición se ha presentado en el contexto de un proceso penal incoado contra H. K. por los cargos de robo, utilización de la tarjeta bancaria de un tercero y violencia contra los intervinientes en un procedimiento judicial.

Marco jurídico

Derecho de la Unión

3 Los considerandos 2 y 11 de la Directiva 2002/58 son del siguiente tenor:

«(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/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)], la presente Directiva no aborda la protección de los derechos y las libertades fundamentales en relación con las actividades no regidas por el Derecho [de la Unión]. 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 [, hecho en Roma el 4 de noviembre de 1950], 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.»

4 Según el artículo 2 de la Directiva 2002/58, con el epígrafe «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:

a) “usuario”: una persona física que utiliza con fines privados o comerciales un servicio de comunicaciones electrónicas disponible para el público, sin que necesariamente se haya abonado a dicho servicio;

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;

[…]».

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

[…]

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]. Lo anterior no impedirá el posible almacenamiento o acceso de índole técnica al solo fin de efectuar la transmisión de una comunicación a través de una red de comunicaciones electrónicas, o en la medida de lo estrictamente necesario a fin de que el proveedor de un servicio de la sociedad de la información preste un servicio expresamente solicitado por el abonado o el usuario.»

6 El artículo 6 de la Directiva 2002/58, bajo la rúbrica «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 [sean necesarios] 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.

3. El proveedor de un servicio de comunicaciones electrónicas disponible para el público podrá tratar los datos a que se hace referencia en el apartado 1 para la promoción comercial de servicios de comunicaciones electrónicas o para la prestación de servicios con valor añadido en la medida y durante el tiempo necesarios para tales servicios o promoción comercial, siempre y cuando el abonado o usuario al que se refieran los datos haya dado su consentimiento previo. Los usuarios o abonados dispondrán de la posibilidad de retirar su consentimiento para el tratamiento de los datos de tráfico en cualquier momento.

[…]

5. Solo podrán encargarse del tratamiento de datos de tráfico, de conformidad con los apartados 1, 2, 3 y 4, las personas que actúen bajo la autoridad del proveedor de las redes públicas de comunicaciones o de servicios de comunicaciones electrónicas disponibles al público que se ocupen de la facturación o de la gestión del tráfico, de las solicitudes de información de los clientes, de la detección de fraudes, de la promoción comercial de los servicios de comunicaciones electrónicas o de la prestación de un servicio con valor añadido, y dicho tratamiento deberá limitarse a lo necesario para realizar tales actividades.

[…]»

7 El artículo 9 de la Directiva 2002/58, titulado «Datos de localización distintos de los datos de tráfico», establece en su apartado 1:

«En caso de que puedan tratarse datos de localización, distintos de los datos de tráfico, relativos a los usuarios o abonados de redes públicas de comunicaciones o de servicios de comunicaciones electrónicas disponibles al público, solo podrán tratarse estos datos si se hacen anónimos, o previo consentimiento de los usuarios o abonados, en la medida y por el tiempo necesarios para la prestación de un servicio con valor añadido. El proveedor del servicio deberá informar a los usuarios o abonados, antes de obtener su consentimiento, del tipo de datos de localización distintos de los datos de tráfico que serán tratados, de la finalidad y duración del tratamiento y de si los datos se transmitirán a un tercero a efectos de la prestación del servicio con valor añadido […]».

8 El artículo 15 de la mencionada Directiva, con el epígrafe «Aplicación de determinadas disposiciones de la Directiva [95/46]», enuncia 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 [de la Unión], incluidos los mencionados en los apartados 1 y 2 del artículo 6 del Tratado de la Unión Europea.»

Derecho estonio

Ley de Comunicaciones Electrónicas

9 El artículo 111[1] de la elektroonilise side seadus (Ley de Comunicaciones Electrónicas) (RT I 2004, 87, 593; RT I, 22.05.2018, 3), en su versión aplicable a los hechos del litigio principal (en lo sucesivo, «Ley de Comunicaciones Electrónicas»), titulado «Obligación de conservar datos», establece:

«[…]

(2) Los proveedores de servicios de telefonía fija y móvil, así como de servicios de red de telefonía fija y móvil, estarán obligados a conservar los datos siguientes:

1) El número de la línea que efectúa la llamada, así como el nombre y la dirección del abonado.

2) El número de la línea que recibe la llamada, así como el nombre y la dirección del abonado.

3) Cuando se utilice un servicio suplementario, como el desvío o la transferencia de llamadas: el número marcado, así como el nombre y la dirección del abonado.

4) La fecha y hora del inicio y de la finalización de la llamada.

5) El servicio de telefonía fija o móvil utilizado.

6) La identidad internacional del abonado móvil (*International Mobile Subscriber Identity* — IMSI) de las líneas que efectúan y reciben la llamada.

7) La identidad internacional del equipo móvil (*International Mobile Equipment Identity* — IMEI) de las líneas que efectúan y reciben la llamada.

8) El identificador de celda al inicio de la llamada.

9) Datos que permitan fijar la localización geográfica de la celda, mediante referencia a su identificador de localización, durante el período en el que se conserven los datos.

10) En el caso de los servicios anónimos de telefonía móvil de pago por adelantado: la fecha y hora de la primera activación del servicio y la etiqueta de localización desde la que se haya activado el servicio.

[…]

(4) Los datos mencionados en los apartados 2 y 3 del presente artículo serán conservados durante un período de un año a partir del momento de la comunicación, si dichos datos fueron generados o tratados en el curso de la prestación de un servicio de comunicación. […]

[…]

(11) Los datos mencionados en los apartados 2 y 3 del presente artículo serán entregados:

1) con arreglo a la kriminaalmenetluse seadustik [(Ley de Enjuiciamiento Criminal),] a la autoridad investigadora, a un organismo autorizado para realizar medidas de vigilancia, al Ministerio Fiscal y al órgano jurisdiccional;

[…]».

Ley de Enjuiciamiento Criminal

10 El artículo 17 de la kriminaalmenetluse seadustik (Ley de Enjuiciamiento Criminal) (RT I 2003, 27, 166; RT I, 31.05.2018, 22) dispone:

«(1) Son partes en el procedimiento judicial: el Ministerio Fiscal, […]

[…]».

11 El artículo 30 de esta Ley tiene el siguiente tenor:

«(1) El Ministerio Fiscal dirige el procedimiento de instrucción, garantizando su legalidad y eficacia, y ejerce la acusación pública ante el órgano jurisdiccional.

(2) Las competencias del Ministerio Fiscal en un procedimiento penal son ejercidas en su nombre por un fiscal que actuará con independencia y que solo estará sometido a la ley.»

12 El artículo 90[1] de dicha Ley establece:

«[…]

(2) La autoridad investigadora podrá, con la autorización del Ministerio Fiscal en el procedimiento de instrucción o del órgano jurisdiccional en el procedimiento judicial, solicitar a un proveedor de servicios de comunicaciones electrónicas los datos enumerados en el artículo 111[1], apartados 2 y 3, de la Ley de Comunicaciones Electrónicas que no se mencionan en el apartado 1 del presente artículo. En la autorización se indicará, con fechas exactas, el período para el que se pueden solicitar los datos.

(3) Conforme al presente artículo, los datos solamente podrán ser solicitados si ello resulta indispensable para alcanzar el objetivo del procedimiento penal.»

13 El artículo 211 de la misma Ley dispone:

«(1) El objetivo del procedimiento de instrucción es reunir pruebas y establecer las demás condiciones para la apertura del juicio oral.

(2) Durante el procedimiento de instrucción, la autoridad investigadora y el Ministerio Fiscal esclarecerán las circunstancias de cargo y de descargo del investigado o acusado.»

Ley del Ministerio Fiscal

14 El artículo 1 de la prokuratuuriseadus (Ley del Ministerio Fiscal) (RT I 1998, 41, 625; RT I, 06.07.2018, 20), en su versión aplicable a los hechos del litigio principal, establece:

«(1) El Ministerio Fiscal es una autoridad adscrita al ámbito de competencia del Ministerio de Justicia, que participa en la planificación de las medidas de vigilancia necesarias para luchar contra la delincuencia y esclarecer los delitos, que dirige el procedimiento de instrucción, garantizando su legalidad y eficacia, y que ejerce la acusación pública ante el órgano jurisdiccional y cumple las demás tareas que le atribuya la ley.

(1[1]) El Ministerio Fiscal ejercerá de manera independiente las funciones que le encomienda la normativa y actuará con arreglo a esta Ley, a las demás leyes y a los actos normativos aprobados sobre la base de dichas leyes.

[…]»

15 El artículo 2, apartado 2, de esta Ley dispone:

«El fiscal ejercerá sus funciones de manera independiente y actuará únicamente de conformidad con la ley y su convicción.»

Litigio principal y cuestiones prejudiciales

16 Mediante resolución de 6 de abril de 2017, H. K. fue condenada por el Viru Maakohus (Tribunal de Primera Instancia de Viru, Estonia) a una pena privativa de libertad de dos años por la comisión, entre el 17 de enero de 2015 y el 1 de febrero de 2016, de varios robos de bienes (de un valor de entre 3 y 40 euros) y de dinero en efectivo (por importes de entre 5,20 y 2 100 euros), por la

utilización de la tarjeta bancaria de un tercero, causándole un perjuicio de 3 941,82 euros, y por la comisión de actos constitutivos de violencia contra los intervinientes en un procedimiento judicial que la afectaba.

17 Para condenar a H. K. por tales hechos, el Viru Maakohus (Tribunal de Primera Instancia de Viru) se basó, entre otros, en varios atestados confeccionados a partir de datos relativos a las comunicaciones electrónicas, con arreglo al artículo 111[1], apartado 2, de la Ley de Comunicaciones Electrónicas, recabados por la autoridad investigadora de un proveedor de servicios de telecomunicaciones electrónicas durante el procedimiento de instrucción, después de haber obtenido varias autorizaciones al efecto del Viru Ringkonnaprokuratuur (Fiscalía de Distrito de Viru, Estonia), de conformidad con el artículo 90[1] de la Ley de Enjuiciamiento Criminal. Estas autorizaciones, concedidas el 28 de enero y el 2 de febrero de 2015, el 2 de noviembre de 2015 y el 25 de febrero de 2016, se referían a datos relativos a varios números de teléfono de H. K. y a distintas identidades internacionales del equipo móvil de esta, respecto al período comprendido entre el 1 de enero y el 2 de febrero de 2015, al 21 de septiembre de 2015, y al período comprendido entre el 1 de marzo de 2015 y el 19 de febrero de 2016.

18 H. K. recurrió en apelación la resolución del Viru Maakohus (Tribunal de Primera Instancia de Viru) ante el Tartu Ringkonnakohus (Tribunal de Apelación de Tartu, Estonia), que desestimó dicho recurso mediante resolución de 17 de noviembre de 2017.

19 H. K. interpuso recurso de casación contra esta última resolución ante el Riigikohus (Tribunal Supremo, Estonia), refutando, entre otras cosas, la admisibilidad de los atestados confeccionados a partir de los datos recabados del proveedor de servicios de comunicaciones electrónicas. Considera que de la sentencia de 21 de diciembre de 2016, Tele2 Sverige y Watson y otros (C-203/15 y C-698/15, en lo sucesivo, «sentencia Tele2», EU:C:2016:970), resulta que las disposiciones del artículo 111[1] de la Ley de Comunicaciones Electrónicas que imponen a los proveedores de servicios la obligación de conservar los datos relativos a las comunicaciones, así como el uso de estos datos a efectos de su condena, son contrarios al artículo 15, apartado 1, de la Directiva 2002/58, interpretado a la luz de los artículos 7, 8, 11 y 52, apartado 1, de la Carta.

20 Según el tribunal remitente, se suscita la cuestión de si los atestados redactados sobre la base de los datos contemplados en el artículo 111[1], apartado 2, de la Ley de Comunicaciones Electrónicas pueden considerarse pruebas admisibles. Dicho tribunal observa que la admisibilidad como pruebas de los atestados controvertidos en el procedimiento principal depende de en qué medida era conforme con el artículo 15, apartado 1, de la Directiva 2002/58, interpretado a la luz de los artículos 7, 8, 11 y 52, apartado 1, de la Carta, recabar los datos a partir de los que se redactaron esos atestados.

21 Dicho tribunal considera que la respuesta a esta cuestión implica determinar si el citado artículo 15, apartado 1, a la luz de la Carta, debe interpretarse en el sentido de que el acceso de las autoridades nacionales a datos que permitan identificar el origen y el destino de una comunicación por teléfono fijo o móvil de un investigado, determinar la fecha, la hora, la duración y la naturaleza de dicha comunicación, identificar el equipo de comunicación utilizado, y localizar el equipo de comunicación móvil utilizado representa una injerencia de tal gravedad en los derechos fundamentales en cuestión que dicho acceso debe limitarse a la lucha contra la delincuencia grave, con independencia del período para el que las autoridades nacionales hayan solicitado acceder a los datos conservados.

22 No obstante, el órgano jurisdiccional remitente considera que la duración de ese período es un elemento esencial a la hora de evaluar la gravedad de la injerencia consistente en acceder a los datos de tráfico y de localización. Así, cuando dicho período es muy breve o la cantidad de datos recogidos es muy limitada, hay que preguntarse si el objetivo de lucha contra la delincuencia en general, y no solo de lucha contra la delincuencia grave, puede justificar tal injerencia.

23 Por último, el tribunal remitente alberga dudas sobre la posibilidad de considerar al Ministerio Fiscal estonio una autoridad administrativa independiente, en el sentido del apartado 120 de la sentencia Tele2, que pueda autorizar el acceso de la autoridad investigadora a datos relativos a las comunicaciones electrónicas como los contemplados en el artículo 111[1], apartado 2, de la Ley de Comunicaciones Electrónicas.

24 El Ministerio Fiscal dirige el procedimiento de instrucción y garantiza su legalidad y eficacia. Dado que el objetivo de dicho procedimiento es, especialmente, recoger pruebas, la autoridad investigadora y el Ministerio Fiscal esclarecen las circunstancias de cargo y de descargo de todo investigado o acusado. Si el Ministerio Fiscal está convencido de que se han recabado todas las pruebas necesarias, ejerce la acusación pública contra el encausado. Las competencias del Ministerio Fiscal son ejercidas en su nombre por un fiscal, que cumple sus funciones con independencia, como resulta del artículo 30, apartados 1 y 2, de la Ley de Enjuiciamiento Criminal y de los artículos 1 y 2 de la Ley del Ministerio Fiscal.

25 En ese contexto, el órgano jurisdiccional remitente indica que sus dudas sobre la independencia exigida por el Derecho de la Unión obedecen principalmente a que el Ministerio Fiscal no solo dirige el procedimiento de instrucción, sino que también ejerce la acusación pública ante el órgano jurisdiccional, ya que dicha autoridad, en virtud del Derecho nacional, es parte en el procedimiento penal.

26 En estas circunstancias, el Riigikohus (Tribunal Supremo) decidió suspender el procedimiento y plantear al Tribunal de Justicia las siguientes cuestiones prejudiciales:

«1) ¿Debe interpretarse el artículo 15, apartado 1, de la Directiva [2002/58], a la luz de los artículos 7, 8, 11 y 52, apartado 1, de la [Carta], en el sentido de que, en el marco de un procedimiento penal, el acceso de las autoridades del Estado a los datos que permiten rastrear e identificar el origen y el destino de una comunicación por teléfono fijo o móvil de un investigado, determinar la fecha, la hora, la duración y la naturaleza de dicha comunicación, identificar el equipo de comunicación utilizado y localizar el equipo de comunicación móvil utilizado representa una injerencia tan grave en los derechos fundamentales consagrados en los artículos antes mencionados de la Carta que dicho acceso, en el ámbito de la prevención, la investigación, el descubrimiento y la persecución de delitos, debe limitarse a la lucha contra la delincuencia grave, con independencia del período a que se refieran los datos conservados a los que tengan acceso las autoridades del Estado?

2) ¿Debe interpretarse el artículo 15, apartado 1, de la Directiva [2002/58] partiendo del principio de proporcionalidad recogido en la [sentencia de 2 de octubre de 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788)], apartados 55 a 57, en el sentido de que, si la cantidad de datos a los que tienen acceso las autoridades del Estado a los que se hace referencia en la primera cuestión prejudicial no es grande (ni por la naturaleza de los datos ni por su extensión temporal), la injerencia que ello implica en los derechos fundamentales puede estar justificada en general por el objetivo de la prevención, la investigación, el descubrimiento y la persecución de delitos, y de que los delitos contra los que se pretenda luchar mediante la injerencia deberán ser de mayor gravedad cuanto mayor sea la cantidad de datos a los que tengan acceso las autoridades del Estado?

3) ¿Significa el requisito mencionado en la [sentencia Tele2], punto 2 del fallo, de que el acceso de las autoridades competentes del Estado a los datos debe estar supeditado a un control previo por un órgano jurisdiccional o una autoridad administrativa independiente que el artículo 15, apartado 1, de la Directiva [2002/58] deba interpretarse en el sentido de que el Ministerio Fiscal, que dirige el procedimiento de instrucción, que al hacerlo está obligado por ley a actuar con independencia y solo está sometido a la ley, y que en el procedimiento de instrucción esclarece tanto las circunstancias de cargo como las de descargo del acusado, pero que posteriormente ejerce la acusación pública en el procedimiento judicial, puede tener la consideración de autoridad administrativa independiente?»

Sobre las cuestiones prejudiciales

Cuestiones prejudiciales primera y segunda

27 Mediante sus dos primeras cuestiones prejudiciales, que procede examinar conjuntamente, el tribunal 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 una normativa nacional que autoriza el acceso de autoridades públicas a un conjunto de datos de tráfico o de localización que pueden facilitar información sobre las comunicaciones efectuadas por un usuario de un medio de comunicación electrónica o sobre la localización de los equipos terminales que utilice y permitir extraer conclusiones precisas sobre su vida privada, a efectos de la prevención, la investigación, el descubrimiento y la persecución de delitos, sin que dicho acceso se limite a procedimientos que tengan por objeto la lucha contra la delincuencia grave, y ello con independencia de la duración del período para el que se solicite acceder a los citados datos y de la cantidad y naturaleza de los datos disponibles en ese período.

28 A este respecto, de la petición de decisión prejudicial resulta, como confirmó el Gobierno estonio en la vista, que los datos a los que tuvo acceso la autoridad investigadora nacional en el litigio principal son los conservados con arreglo al artículo 111[1], apartados 2 y 4, de la Ley de Comunicaciones Electrónicas, que obliga a los proveedores de servicios de comunicaciones electrónicas a la conservación generalizada e indiferenciada de los datos de tráfico y de localización relativos a la telefonía fija y móvil durante un año. Estos datos permiten, entre otras cosas, rastrear e identificar el origen y el destino de una comunicación por teléfono fijo o móvil de una persona, determinar la fecha, la hora, la duración y la naturaleza de dicha comunicación, identificar el equipo de comunicación utilizado y localizar el teléfono móvil, sin que se transmita necesariamente la comunicación. Además, ofrecen la posibilidad de determinar la frecuencia de las comunicaciones del usuario con determinadas personas durante un período concreto. Por otra parte, como confirmó el Gobierno estonio en la vista, el acceso a dichos datos puede solicitarse, en materia de lucha contra la delincuencia, para cualquier tipo de delito.

29 Por lo que respecta a las condiciones en las que puede concederse el acceso a los datos de tráfico y de localización conservados por los proveedores de servicios de comunicaciones electrónicas, a efectos de la prevención, la investigación, el descubrimiento y la persecución de delitos, a las autoridades públicas con arreglo a una medida adoptada al amparo del artículo 15, apartado 1, de la Directiva 2002/58, el Tribunal de Justicia ha declarado que dicho acceso solo puede concederse para el caso de que esos datos hayan sido conservados por tales proveedores de conformidad con el citado artículo 15, apartado 1 (véase, en este sentido, la 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 167).

30 El Tribunal de Justicia también ha señalado al respecto que dicho artículo 15, apartado 1, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta, se opone a medidas legislativas que establezcan, para tales fines, con carácter preventivo, la conservación generalizada e indiferenciada de los datos de tráfico y de localización (véase, en este sentido, la 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 168).

31 En cuanto a los objetivos que pueden justificar el acceso de las autoridades públicas a los datos conservados por los proveedores de servicios de comunicaciones electrónicas con arreglo a una medida conforme con esas disposiciones, de la jurisprudencia del Tribunal de Justicia se desprende, por una parte, que tal acceso solo puede estar justificado por el objetivo de interés general para el que dicha conservación se impuso a los citados proveedores de servicios (véase, en este sentido, la 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 166).

32 Por otra parte, el Tribunal de Justicia ha declarado que 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 y jurisprudencia citada).

33 En lo que atañe al objetivo de prevención, investigación, descubrimiento y persecución de delitos pretendido por la normativa controvertida en el litigio principal, 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. 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 pretendido por la normativa controvertida en el litigio principal (véase, en este sentido, la 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, apartados 140 y 146).

34 En particular, se ha declarado al respecto que las medidas legislativas relativas al tratamiento de datos referidos a la identidad civil de los usuarios de los medios de comunicaciones electrónicas como tales, en particular a su conservación y al acceso a los mismos, con el único objetivo de identificar al usuario de que se trate, y sin que dichos datos puedan vincularse a informaciones relativas a las comunicaciones efectuadas, pueden estar justificadas 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. En efecto, dichos datos no permiten, por sí solos, conocer la fecha, la hora, la duración y los destinatarios de las comunicaciones efectuadas, ni los lugares en los que se produjeron estas comunicaciones o la frecuencia de las mismas con ciertas personas durante un período de tiempo determinado, por lo que no facilitan, al margen de las coordenadas de los usuarios de los medios de comunicaciones electrónicas, como sus direcciones, ninguna información sobre las comunicaciones transmitidas y, en consecuencia, sobre su vida privada. De este modo, la injerencia que supone una medida relativa a estos datos no puede, en principio, calificarse de grave (véase, en este sentido, la 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, apartados 157 y 158 y jurisprudencia citada).

35 En estas circunstancias, solo los objetivos de lucha contra la delincuencia grave o de prevención de las amenazas graves contra la seguridad pública pueden justificar el acceso de las autoridades públicas a un conjunto de datos de tráfico o de localización que puedan facilitar información sobre las comunicaciones efectuadas por un usuario de un medio de comunicación electrónica o sobre la localización de los equipos terminales que utilice que permitan extraer conclusiones precisas sobre la vida privada de las personas afectadas (véase, en este sentido, la sentencia de 2 de octubre de 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, apartado 54), sin que otros factores relativos a la proporcionalidad de la solicitud de acceso, como la duración del período para el que se solicita el acceso a tales datos, puedan conllevar que el objetivo de prevención, investigación, descubrimiento y persecución de delitos en general justifique tal acceso.

36 Procede señalar que el acceso a un conjunto de datos de tráfico o de localización como los conservados en virtud del artículo 111[1] de la Ley de Comunicaciones Electrónicas efectivamente puede permitir extraer conclusiones precisas —incluso muy precisas— sobre la vida privada de las personas cuyos datos se han conservado, como los hábitos de la vida cotidiana, los lugares de residencia permanentes o temporales, los desplazamientos diarios u otros, las actividades realizadas, sus relaciones sociales y los círculos sociales que frecuentan (véase, en este sentido, la 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 117).

37 Como sugiere el tribunal remitente, es cierto que, cuanto mayor sea el período para el que se solicite el acceso, mayor es, en principio, la cantidad de datos que pueden conservar los proveedores de servicios de comunicaciones electrónicas relativos a antiguas comunicaciones electrónicas, a los lugares de residencia frecuentados y a los desplazamientos realizados por el usuario de un medio de comunicación electrónica, lo que permite extraer, a partir de los datos consultados, más conclusiones sobre la vida privada de dicho usuario. Análoga conclusión puede extraerse en cuanto a las categorías de datos solicitados.

38 Por consiguiente, para cumplir el requisito de proporcionalidad, según el cual las excepciones a la protección de los datos personales y las restricciones a dicha protección deben establecerse sin sobrepasar los límites de lo estrictamente necesario (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 130 y jurisprudencia citada), corresponde a las autoridades nacionales competentes garantizar, en cada supuesto, que tanto las categorías de datos contemplados como la duración para la que se solicita el acceso a los mismos se limiten, en función de las circunstancias del caso, a lo estrictamente necesario a efectos de la investigación de que se trate.

39 No obstante, la injerencia en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta que supone el acceso por parte de una autoridad pública a un conjunto de datos de tráfico o de localización que pueden facilitar información sobre las comunicaciones efectuadas por un usuario de un medio de comunicación electrónica o sobre la localización de los equipos terminales que utilice es, en todo caso, grave, con independencia de la duración del período para el que se solicite el acceso a dichos datos y de la cantidad o naturaleza de los datos disponibles en ese período, cuando, al igual que ocurre en el litigio principal, ese conjunto de datos pueda permitir extraer conclusiones precisas sobre la vida privada de las personas afectadas.

40 A este respecto, incluso el acceso a una cantidad limitada de datos de tráfico o de localización o el acceso a datos durante un período breve puede facilitar información precisa sobre la vida privada de un usuario de un medio de comunicación electrónica. Además, la cantidad de datos disponibles y la información concreta sobre la vida privada de la persona afectada que de ellos resulta son circunstancias que solo pueden apreciarse después de consultar dichos datos. Sin embargo, la autorización de acceso del órgano jurisdiccional o de la autoridad independiente competente se concede necesariamente antes de que se puedan consultar los datos y la información que se deriva de ellos. Así, la apreciación de la gravedad de la injerencia del acceso se efectúa necesariamente en función del riesgo para la vida privada de las personas afectadas que suele corresponder a la categoría de datos solicitados, sin que, por otra parte, sea preciso saber si la información relativa a la vida privada que de ellos deriva es, en concreto, sensible o no.

41 Por último, habida cuenta de que el tribunal remitente conoce de una pretensión en la que se solicita la inadmisión de los atestados confeccionados a partir de los datos de tráfico y de localización, debido a que las disposiciones del artículo 111^{1} de la Ley de Comunicaciones Electrónicas supuestamente son contrarias al artículo 15, apartado 1, de la Directiva 2002/58 tanto en lo relativo a la conservación de los datos como en cuanto al acceso a los mismos, procede recordar que, en el estado actual del Derecho de la Unión, incumbe en principio únicamente al Derecho nacional determinar las normas relativas a la admisibilidad y a la apreciación, en el marco de un proceso penal incoado contra personas sospechosas de haber cometido actos de delincuencia, de la información y de las pruebas que se han obtenido mediante una conservación generalizada e indiferenciada de tales datos contraria al Derecho de la Unión (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 222), o incluso mediante un acceso de las autoridades nacionales a dichos datos contrario a ese Derecho.

42 En efecto, según reiterada jurisprudencia, ante la inexistencia de normas de la Unión en la materia, corresponde al ordenamiento jurídico interno de cada Estado miembro, en virtud del principio de autonomía procesal, configurar la regulación procesal de los recursos destinados a garantizar la

salvaguardia de los derechos que el Derecho de la Unión confiere a los justiciables, a condición, sin embargo, de que no sea menos favorable que la que rige situaciones similares de carácter interno (principio de equivalencia) y de que no haga imposible en la práctica o excesivamente difícil el ejercicio de los derechos conferidos por el Derecho de la Unión (principio de efectividad) (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 223 y jurisprudencia citada).

43 Por lo que respecta, más concretamente, al principio de efectividad, es preciso recordar que las normas nacionales relativas a la admisibilidad y al uso de la información y las pruebas tienen como objetivo, en virtud de las elecciones efectuadas por el Derecho nacional, evitar que la información y las pruebas que se han obtenido de manera ilegal perjudiquen indebidamente a una persona sospechosa de haber cometido delitos. Pues bien, con arreglo al Derecho nacional, este objetivo puede alcanzarse, además de mediante una prohibición de utilizar dicha información y dichas pruebas, mediante normas y prácticas nacionales que regulen la apreciación y la ponderación de la información y las pruebas, o incluso mediante la consideración de su carácter ilegal en el marco de la determinación de la pena (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 225).

44 La necesidad de excluir la información y las pruebas obtenidas incumpliendo lo dispuesto en el Derecho de la Unión debe apreciarse atendiendo, en particular, al riesgo que la admisibilidad de dicha información y de dichas pruebas supone para el respeto del principio de contradicción y, por lo tanto, del derecho a un juicio justo. Pues bien, un órgano jurisdiccional que considera que una parte no está en condiciones de comentar eficazmente un medio de prueba que pertenece a un ámbito que escapa al conocimiento de los jueces y que puede influir destacadamente en la apreciación de los hechos debe declarar que existe una violación del derecho a un juicio justo y excluir ese medio de prueba a fin de evitar una violación de esta índole. En consecuencia, el principio de efectividad exige al juez penal nacional que descarte la información y las pruebas que se han obtenido a través de una conservación generalizada e indiferenciada de los datos de tráfico y de localización incompatible con el Derecho de la Unión o incluso mediante el acceso de la autoridad competente a esos datos infringiendo dicho Derecho, en el marco de un proceso penal incoado contra personas sospechosas de haber cometido actos de delincuencia, cuando estas personas no estén en condiciones de comentar eficazmente tal información y tales pruebas, que proceden de un ámbito que escapa al conocimiento de los jueces y que pueden influir destacadamente en la apreciación de los hechos (véase, en este sentido, la 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, apartados 226 y 227).

45 Habida cuenta de las consideraciones anteriores, procede responder a las dos primeras cuestiones prejudiciales 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 una normativa nacional que autoriza el acceso de autoridades públicas a un conjunto de datos de tráfico o de localización que pueden facilitar información sobre las comunicaciones efectuadas por un usuario de un medio de comunicación electrónica o sobre la localización de los equipos terminales que utilice y permitir extraer conclusiones precisas sobre su vida privada, a efectos de la prevención, la investigación, el descubrimiento y la persecución de delitos, sin que dicho acceso se limite a procedimientos que tengan por objeto la lucha contra la delincuencia grave o la prevención de amenazas graves contra la seguridad pública, y ello con independencia de la duración del período para el que se solicite acceder a los citados datos y de la cantidad o naturaleza de los datos disponibles en ese período.

Tercera cuestión prejudicial

46 Mediante su tercera cuestión prejudicial, el tribunal 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 una normativa nacional que atribuye competencia al Ministerio Fiscal —cuya función es dirigir el procedimiento de instrucción penal y ejercer, en su caso, la acusación pública en un procedimiento posterior— para autorizar el acceso de una autoridad pública a los datos de tráfico y de localización a efectos de la instrucción penal.

47 El tribunal remitente precisa a este respecto que, si bien el Ministerio Fiscal estonio, de conformidad con el Derecho nacional, está obligado a actuar de manera independiente, está sometido únicamente a la ley y debe examinar las circunstancias de cargo y de descargo en el procedimiento de instrucción, no es menos cierto que el objetivo de este procedimiento es reunir pruebas y establecer las demás condiciones para la apertura del juicio oral. Esta misma autoridad ejerce la acusación pública ante el órgano jurisdiccional, por lo que también es parte en el procedimiento judicial. Además, de los autos que obran en poder del Tribunal de Justicia se desprende, como también confirmaron el Gobierno estonio y el Prokuratuur en la vista, que el Ministerio Fiscal estonio se organiza jerárquicamente y que las solicitudes de acceso a los datos de tráfico y de localización no están sometidas a ningún requisito de forma concreto y pueden ser presentadas por el propio fiscal. Por último, las personas a cuyos datos se puede autorizar el acceso no son únicamente las sospechosas de estar implicadas en un delito.

48 Es cierto, como ya ha declarado el Tribunal de Justicia, que corresponde al Derecho nacional determinar los requisitos con arreglo a los cuales los proveedores de servicios de comunicaciones electrónicas deben conceder a las autoridades nacionales competentes acceso a los datos de que disponen. No obstante, para cumplir el requisito de proporcionalidad, una normativa de este tipo debe establecer reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión e impongan unas exigencias mínimas, de modo que las personas cuyos datos personales resulten afectados dispongan de garantías suficientes que permitan proteger de manera eficaz esos datos contra los riesgos de abuso. Dicha normativa debe ser legalmente imperativa en Derecho interno e indicar en qué circunstancias y con arreglo a qué requisitos puede adoptarse una medida que contemple el tratamiento de tales datos, garantizando así que la injerencia se limite a lo estrictamente necesario (véanse, en este sentido, las sentencias Tele2, apartados 117 y 118; de 6 de octubre de 2020, Privacy International, C-623/17, EU:C:2020:790, apartado 68, y 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 132 y jurisprudencia citada).

49 En particular, una normativa nacional que regula el acceso de las autoridades competentes a los datos de tráfico y de localización conservados, adoptada en virtud del artículo 15, apartado 1, de la Directiva 2002/58, no puede limitarse a exigir que el acceso de las autoridades a los datos responda a la finalidad perseguida por dicha normativa, sino que debe establecer también los requisitos materiales y procedimentales que regulen la referida utilización (sentencias de 6 de octubre de 2020, Privacy International, C-623/17, EU:C:2020:790, apartado 77, y 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 176 y jurisprudencia citada).

50 De este modo, y puesto que un acceso general a todos los datos conservados, con independencia de la existencia de una relación, por lo menos indirecta, con el fin perseguido, no puede considerarse limitado a lo estrictamente necesario, la normativa nacional de que se trate debe basarse en criterios objetivos para definir las circunstancias y los requisitos conforme a los cuales debe concederse a las autoridades nacionales competentes el acceso a los datos en cuestión. A este respecto, en principio solo podrá concederse un acceso de este tipo en relación con el objetivo de la lucha contra la delincuencia a los datos de personas de las que se sospeche que planean, van a cometer o han cometido un delito grave o que puedan estar implicadas de un modo u otro en un delito grave. No obstante, en situaciones particulares, como aquellas en las que intereses vitales de la seguridad nacional, la defensa o la seguridad pública estén amenazados por actividades terroristas, podría igualmente concederse el acceso a los datos de otras personas cuando existan elementos objetivos que

permitan considerar que esos datos podrían, en un caso concreto, contribuir de modo efectivo a la lucha contra dichas actividades (véanse, en este sentido, las sentencias Tele2, apartado 119, y 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 188).

51 Para garantizar en la práctica el íntegro cumplimiento de estos requisitos, es esencial que el acceso de las autoridades nacionales competentes a los datos conservados se supedite a un control previo efectuado bien por un órgano jurisdiccional, bien por una entidad administrativa independiente, y que la decisión de este órgano jurisdiccional o de esta entidad se dicte a raíz de una solicitud motivada de dichas autoridades presentada, en particular, en el marco de procedimientos de prevención, descubrimiento y persecución de delitos. En caso de urgencia debidamente justificada, el control debe efectuarse en breve plazo (véase, en este sentido, la 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 189 y jurisprudencia citada).

52 Este control previo requiere, entre otras cosas, como indicó, en esencia, el Abogado General en el punto 105 de sus conclusiones, que el órgano jurisdiccional o la entidad encargada de efectuar dicho control previo disponga de todas las atribuciones y presente todas las garantías necesarias para conciliar los diferentes intereses y derechos de que se trate. En el caso concreto de la investigación penal, tal control exige que ese órgano jurisdiccional o esa entidad esté en condiciones de ponderar adecuadamente, por una parte, los intereses relacionados con las necesidades de la investigación en el marco de la lucha contra la delincuencia y, por otra parte, los derechos fundamentales al respeto de la vida privada y a la protección de los datos personales de aquellos a cuyos datos afecte el acceso.

53 Cuando dicho control no lo lleve a cabo un órgano jurisdiccional, sino una entidad administrativa independiente, esta debe gozar de un estatuto que le permita actuar en el ejercicio de sus funciones con objetividad e imparcialidad, y, para ello, ha de estar a resguardo de toda influencia externa [véanse, en este sentido, la sentencia de 9 de marzo de 2010, Comisión/Alemania, C-518/07, EU:C:2010:125, apartado 25, y el dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartados 229 y 230].

54 De las consideraciones anteriores resulta que el requisito de independencia que debe cumplir la autoridad que ejerce el control previo recordado en el apartado 51 de la presente sentencia obliga a que dicha autoridad tenga la condición de tercero respecto de la que solicita el acceso a los datos, de modo que la primera pueda ejercer ese control con objetividad e imparcialidad, y a resguardo de toda influencia externa. En particular, en el ámbito penal, el requisito de independencia implica, como señaló el Abogado General, en esencia, en el punto 126 de sus conclusiones, que la autoridad que ejerce ese control previo, por una parte, no esté implicada en la realización de la investigación penal de que se trate y, por otra parte, que tenga una posición neutral frente a las partes del procedimiento penal.

55 No ocurre así con un Ministerio Fiscal que dirige el procedimiento de investigación y ejerce, en su caso, la acusación pública. En efecto, la función del Ministerio Fiscal no es resolver con total independencia un litigio, sino someterlo, en su caso, al órgano jurisdiccional competente, como parte en el proceso que ejerce la acusación penal.

56 El hecho de que el Ministerio Fiscal, de conformidad con la normativa que regula sus competencias y su estatuto, esté obligado a esclarecer las circunstancias de cargo y de descargo, a garantizar la legalidad del procedimiento de instrucción y a actuar únicamente de conformidad con la ley y su convicción no basta para conferirle el estatuto de tercero con respecto a los intereses controvertidos en el sentido descrito en el apartado 52 de la presente sentencia.

57 De ello se deduce que el Ministerio Fiscal no puede llevar a cabo el control previo mencionado en el apartado 51 de la presente sentencia.

58 Por otra parte, dado que el tribunal remitente ha planteado la cuestión de si cabe suplir la falta de control que lleva a cabo una autoridad independiente por el control posterior que ejerce un órgano jurisdiccional de la legalidad del acceso de una autoridad nacional a los datos de tráfico y de localización, es preciso señalar que el control independiente debe realizarse, como exige la jurisprudencia recordada en el apartado 51 de la presente sentencia, antes de cualquier acceso, salvo en caso de urgencia debidamente justificada, supuesto en el cual el control debe efectuarse en breve plazo. Como indicó el Abogado General en el punto 128 de sus conclusiones, ese control posterior incumple el objetivo del control previo, que consiste en impedir que se autorice un acceso a los datos de que se trate que exceda de los límites de lo estrictamente necesario.

59 En estas circunstancias, procede responder a la tercera cuestión prejudicial 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 una normativa nacional que atribuye competencia al Ministerio Fiscal —cuya función es dirigir el procedimiento de instrucción penal y ejercer, en su caso, la acusación pública en un procedimiento posterior— para autorizar el acceso de una autoridad pública a los datos de tráfico y de localización a efectos de la instrucción penal.

Costas

60 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:

1) **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, debe interpretarse en el sentido de que se opone a una normativa nacional que autoriza el acceso de autoridades públicas a un conjunto de datos de tráfico o de localización que pueden facilitar información sobre las comunicaciones efectuadas por un usuario de un medio de comunicación electrónica o sobre la localización de los equipos terminales que utilice y permitir extraer conclusiones precisas sobre su vida privada, a efectos de la prevención, la investigación, el descubrimiento y la persecución de delitos, sin que dicho acceso se limite a procedimientos que tengan por objeto la lucha contra la delincuencia grave o la prevención de amenazas graves contra la seguridad pública, y ello con independencia de la duración del período para el que se solicite acceder a los citados datos y de la cantidad o naturaleza de los datos disponibles en ese período.**

2) **El artículo 15, apartado 1, de la Directiva 2002/58, en su versión modificada por la Directiva 2009/136, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta de los Derechos Fundamentales, debe interpretarse en el sentido de que se opone a una normativa nacional que atribuye competencia al Ministerio Fiscal —cuya función es dirigir el procedimiento de instrucción penal y ejercer, en su caso, la acusación pública en un procedimiento posterior— para autorizar el acceso de una autoridad pública a los datos de tráfico y de localización a efectos de la instrucción penal.**

Firmas