SENTENCIA DEL TRIBUNAL DE JUSTICIA (Gran Sala)

de 30 de abril de 2024 (*)

«Procedimiento prejudicial — Tratamiento de los datos personales en el sector de las comunicaciones electrónicas — Confidencialidad de las comunicaciones — Proveedores de servicios de comunicaciones electrónicas — Directiva 2002/58/CE — Artículo 15, apartado 1 — Artículos 7, 8, 11 y 52, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea — Acceso a esos datos solicitado por una autoridad nacional competente para el enjuiciamiento de delitos de hurto con circunstancias agravantes — Definición del concepto de "delito grave" cuya persecución puede justificar una injerencia grave en los derechos fundamentales — Competencia de los Estados miembros — Principio de proporcionalidad — Alcance del control previo del juez sobre las solicitudes de acceso a los datos conservados por los proveedores de servicios de comunicaciones electrónicas»

En el asunto C-178/22,

que tiene por objeto una petición de decisión prejudicial planteada, con arreglo al artículo 267 TFUE, por el Giudice delle indagini preliminari presso il Tribunale di Bolzano (Juez de Instrucción del Tribunal de Bolzano, Italia), mediante resolución de 20 de febrero de 2022, recibida en el Tribunal de Justicia el 8 de marzo de 2022, en los procesos penales seguidos contra

Desconocidos,

con intervención de:

Procura della Repubblica presso il Tribunale di Bolzano,

EL TRIBUNAL DE JUSTICIA (Gran Sala),

integrado por el Sr. K. Lenaerts, Presidente, el Sr. L. Bay Larsen, Vicepresidente, el Sr. A. Arabadjiev, las Sras. A. Prechal y K. Jürimäe y los Sres. T. von Danwitz y Z. Csehi, Presidentes de Sala, y los Sres. J.-C. Bonichot, S. Rodin, P. G. Xuereb (Ponente) y D. Gratsias, la Sra. M. L. Arastey Sahún y el Sr. M. Gavalec, Jueces;

Abogado General: Sr. A. M. Collins;

Secretario: Sr. C. Di Bella, administrador;

habiendo considerado los escritos obrantes en autos y celebrada la vista el 21 de marzo de 2023;

consideradas las observaciones presentadas:

– en nombre de la Procura della Repubblica presso il Tribunale di Bolzano, por la Sra. F. Iovene, sostituto procuratore della Repubblica;

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

– en nombre del Gobierno checo, por la Sra. A. Edelmannová, los Sres. O. Serdula y M. Smolek, la Sra. T. Suchá y el Sr. 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, Chief State Solicitor, 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 las Sras. A. Daniel y A.-L. Desjonquères y por los Sres. B. Fodda y J. Illouz, en calidad de agentes;

– en nombre del Gobierno chipriota, por la Sra. E. Neophytou, en calidad de agente;

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

– en nombre del Gobierno neerlandés, por las Sras. M. K. Bulterman y A. Hanje y por el Sr. J. Langer, en calidad de agentes;

– en nombre del Gobierno austriaco, por el Sr. A. Posch, las Sras. J. Schmoll y C. Gabauer, el Sr. K. Ibili y la Sra. E. Samoilova, en calidad de agentes;

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

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

oídas las conclusiones del Abogado General, presentadas en audiencia pública el 8 de junio 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»), 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 una solicitud formulada ante el Giudice delle indagini preliminari presso il Tribunale di Bolzano (Juez de Instrucción del Tribunal de Bolzano, Italia) por la Procura della Repubblica presso il Tribunale di Bolzano (Fiscalía del Tribunal de Bolzano, Italia; en lo sucesivo, «Ministerio Fiscal»), con el fin de que le autorice a acceder a una serie de datos personales conservados por proveedores de servicios de comunicaciones electrónicas para identificar a los autores de dos hurtos de teléfono móvil con circunstancias agravantes.

Marco jurídico

Derecho de la Unión

Directiva 2002/58

3 Los considerandos 2 y 11 de la Directiva 2002/58 enuncian:

«(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 [la Carta].

[…]

(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 comunitario. Por lo tanto, no altera el equilibrio actual entre el derecho de las personas a la intimidad y la posibilidad de que disponen los Estados miembros, según se indica en el apartado 1 del artículo 15 de la presente Directiva, de tomar las medidas necesarias para la protección de la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando las actividades tengan relación con asuntos de seguridad del Estado) y la aplicación del Derecho penal. En consecuencia, la presente Directiva no afecta a la capacidad de los Estados miembros para interceptar legalmente las comunicaciones electrónicas o tomar otras medidas, cuando sea necesario, para cualquiera de estos fines y de conformidad con el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales [, firmado 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 A tenor de lo dispuesto en el artículo 2 de esta Directiva, titulado «Definiciones»:

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

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

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 El artículo 5 de dicha Directiva, cuyo epígrafe es «Confidencialidad de las comunicaciones», establece:

«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 misma Directiva, titulado «Datos de tráfico», dispone:

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

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

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 comunitario, incluidos los mencionados en los apartados 1 y 2 del artículo 6 [TUE].»

Derecho italiano

Decreto Legislativo n.º 196/2003

9 El artículo 132, apartado 3, del Decreto Legislativo n.º 196 — Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n.º 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE [Decreto Legislativo n.º 196, por el que se establece el Código en materia de protección de datos personales, por el que se adapta el Derecho nacional al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE], de 30 de junio de 2003 (suplemento ordinario de la GURI n.º 174, de 29 de julio de 2003), en su redacción aplicable al litigio principal (en lo sucesivo, «Decreto Legislativo n.º 196/2003»), establece lo siguiente:

«Dentro del plazo de conservación impuesto por la ley, si existen indicios suficientes de un delito para el que la ley establezca una pena de prisión permanente o una pena máxima de prisión no inferior a 3 años, determinada de conformidad con el artículo 4 del [codice di procedura penale (Código de Enjuiciamiento Criminal)], y de delitos de amenazas y de acoso u hostigamiento por teléfono contra las personas, si las amenazas, el acoso y el hostigamiento son graves, cuando sea pertinente para la determinación de los hechos, se obtendrán los datos previa autorización del juez mediante auto motivado, a solicitud del Ministerio Fiscal o del abogado del imputado, del investigado, de la víctima y de las otras partes particulares.»

10 A tenor del apartado 3 *bis* de dicho artículo:

«Cuando concurran razones de urgencia y existan motivos fundados para considerar que la demora puede dar lugar a un grave perjuicio para la instrucción, el Ministerio Fiscal ordenará la obtención de datos en virtud de decisión motivada que se comunicará inmediatamente, y en todo caso no más tarde de 48 horas, al juez competente a efectos de la concesión de la autorización en vía ordinaria. El juez decidirá en las 48 horas siguientes sobre su convalidación mediante auto motivado.»

11 Por último, en virtud del apartado 3 *quater*, de dicho artículo, «no podrán utilizarse los datos recogidos contraviniendo las disposiciones establecidas en los apartados 3 y 3 *bis*».

Código Penal

12 El artículo 624 del codice penale (Código Penal), titulado «Hurto», dispone:

«El que, con ánimo de lucro para sí o para terceros, tome las cosas muebles ajenas sin la voluntad de su dueño será castigado con la pena de prisión de seis meses a tres años y con multa de 154 a 516 euros.»

[…]

El delito será punible previa denuncia del perjudicado, a menos que concurran una o varias de las circunstancias mencionadas en los artículos 61, apartado 7, y 625.»

13 El artículo 625, párrafo primero, del Código Penal, titulado «Circunstancias agravantes», establece:

«El hecho mencionado en el artículo 624 será castigado con pena de prisión de dos a seis años y con multa de entre 927 y 1 500 euros:

[…]

2) si el culpable emplea fuerza en las cosas o se vale de cualquier medio fraudulento;

3) si el culpable lleva consigo armas o estupefacientes, sin utilizarlos;

4) si se trata de una conducta caracterizada por una especial astucia o habilidad para aprovechar o provocar la distracción de la víctima;

5) si el hecho es cometido por tres o más personas, o incluso por una sola, disfrazada o que simule la condición de autoridad pública o de persona que ejerza una función pública;

6) si el hecho es cometido sobre el equipaje de viajeros en cualquier tipo de vehículo, en estaciones, aeropuertos o muelles, en hoteles o en cualquier establecimiento que comercialice alimentos o bebidas;

7) si el hecho es cometido sobre bienes presentes en oficinas o establecimientos públicos, o confiscados o incautados, o expuestos por necesidad o por costumbre o por destino a la fe pública, o destinados al servicio público o a la utilidad pública, a la defensa o a la veneración;

7 *bis*) si el hecho es cometido sobre componentes metálicos u otros materiales sustraídos de infraestructuras destinadas al suministro de energía, servicios de transporte, telecomunicaciones u otros servicios públicos y explotados por entidades públicas o privadas en el marco de una concesión pública;

8) si el hecho es cometido sobre tres o más cabezas de ganado agrupadas en rebaño, o sobre animales de las especies bovina o equina, incluso no reunidos en rebaño;

8 *bis*) si el hecho es cometido en medios de transporte público;

8 *ter*) si el hecho es cometido respecto de una persona que esté utilizando o que acabe de utilizar los servicios de una entidad de crédito, de una oficina de correos o de un cajero automático.»

Código de Enjuiciamiento Criminal

14 A tenor del artículo 4 del Código de Enjuiciamiento Criminal, titulado «Normas para la determinación de la competencia»:

«A fin de determinar la competencia se tendrá en cuenta la pena establecida en la ley para cada delito consumado o en grado de tentativa. No se tendrán en cuenta el carácter continuado, la reincidencia ni las circunstancias del delito, con excepción de las circunstancias agravantes para las que la ley establezca una pena de naturaleza distinta de la ordinaria del delito y las que produzcan un efecto especial.»

15 De conformidad con el artículo 269, apartado 2, del referido Código:

«[…] Los registros se conservarán hasta que se dicte sentencia firme. No obstante, para proteger la confidencialidad, cuando los documentos sean irrelevantes a efectos del procedimiento los interesados podrán solicitar al juez que haya autorizado o validado la interceptación la destrucción de las grabaciones.»

Litigio principal y cuestión prejudicial

16 A raíz de dos denuncias presentadas por hurtos de teléfono móvil cometidos el 27 de octubre y el 20 de noviembre de 2021, respectivamente, el Ministerio Fiscal inició, con arreglo a los artículos 624 y 625 del Código Penal, sendos procesos penales contra autores desconocidos por delitos de hurto con circunstancias agravantes.

17 Con el fin de identificar a los autores de dichos hurtos, el Ministerio Fiscal solicitó, sobre la base del artículo 132, apartado 3, del Decreto Legislativo n.º 196/2003, respectivamente los días 7 de diciembre y 30 de diciembre de 2021, al Giudice delle indagini preliminari presso il Tribunale di Bolzano (Juez de Instrucción del Tribunal de Bolzano), órgano jurisdiccional remitente, autorización para recabar de todas las compañías telefónicas los registros telefónicos de los teléfonos sustraídos. Dichas solicitudes se referían a «todos los datos que obren en [poder de las compañías telefónicas], siguiendo un método de rastreo y de localización [en particular, los abonados y, en su caso, los códigos [relativos a la identidad internacional del equipo móvil (IMEI) de los aparatos] de llamadas entrantes o salientes, los sitios visitados y a los que se ha accedido, el momento y la duración de la llamada o de la conexión y la indicación de las partes de redes o repetidores de que se trate, los abonados y los códigos IMEI [de los aparatos] que han enviado y recibido SMS o MMS

y, siempre que sea posible, los datos de identidad de los respectivos titulares] de las conversaciones y comunicaciones telefónicas y de las conexiones efectuadas, incluso en itinerancia, entrantes o salientes, aunque no hayan dado lugar a facturación (llamadas perdidas) desde la fecha del robo hasta la fecha en que se redacte la solicitud».

18 El órgano jurisdiccional remitente alberga dudas en cuanto a la compatibilidad del artículo 132, apartado 3, del Decreto Legislativo n.º 196/2003 con el artículo 15, apartado 1, de la Directiva 2002/58, tal como lo interpretó el Tribunal de Justicia en su 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).

19 Recuerda que, en virtud del apartado 45 de dicha sentencia, no pueden justificarse unas disposiciones nacionales que autoricen el acceso de autoridades públicas a registros telefónicos, que incluyan un conjunto de datos de tráfico o de localización que pueden permitir extraer conclusiones precisas sobre la vida privada del usuario afectado, habida cuenta del principio de proporcionalidad previsto en el artículo 52, apartado 1, de la Carta y de la gravedad de la injerencia en los derechos fundamentales a la vida privada, a la protección de los datos de carácter personal y a la libertad de expresión y de información, tal como se garantizan, respectivamente, en los artículos 7, 8 y 11 de la Carta, a menos que estén destinadas a perseguir delitos graves, como las amenazas graves contra la seguridad pública, entendida como la del Estado, y otras formas de delincuencia grave.

20 A este respecto, el órgano jurisdiccional remitente indica que, en su sentencia n.º 33116 de 7 de septiembre de 2021, la Corte suprema di cassazione (Tribunal Supremo de Casación, Italia) consideró que, habida cuenta del margen de interpretación que rodeaba a la determinación de los delitos que constituyen amenazas graves contra la seguridad pública u otros delitos graves en el sentido de la jurisprudencia del Tribunal de Justicia, esta jurisprudencia no presentaba las características requeridas para ser aplicada directamente por los órganos jurisdiccionales nacionales. Añade que, como consecuencia de ello, el legislador italiano modificó el artículo 132, apartado 3, del Decreto Legislativo n.º 196/2003, con el fin de calificar como delitos graves, para los que pueden obtenerse los extractos telefónicos, los delitos que la ley castiga con una pena privativa de libertad máxima «no inferior a tres años».

21 Según el órgano jurisdiccional remitente, tal umbral de tres años a partir del cual la pena privativa de libertad máxima con que se castiga un delito justifica que ese delito pueda dar lugar a la comunicación de extractos telefónicos a las autoridades públicas podría llevar a que estos registros fueran comunicados para perseguir delitos que solo causan una escasa alarma social y que únicamente se castigan previa denuncia de un particular, en concreto, hurtos de objetos de escaso valor, como los de teléfonos móviles o bicicletas.

22 Considera que, de este modo, la disposición nacional de que se trata vulnera el principio de proporcionalidad establecido en el artículo 52, apartado 1, de la Carta, que exige ponderar la gravedad del delito perseguido con los derechos fundamentales que se ven menoscabados para perseguirlo. En su opinión, este principio se opone a que una vulneración de los derechos fundamentales garantizados por los artículos 7, 8 y 11 de la Carta se justifique por la persecución de un delito como el hurto.

23 El órgano jurisdiccional remitente precisa que los órganos jurisdiccionales italianos disponen de un margen de apreciación muy limitado para denegar la autorización para obtener extractos telefónicos, ya que, en virtud de la disposición controvertida, la autorización debe concederse si existen «indicios suficientes de un delito» y si los datos solicitados son «pertinentes para la determinación de los hechos». Por lo tanto, los órganos jurisdiccionales italianos no disponen de margen de apreciación alguno en cuanto a la gravedad concreta del delito objeto de la investigación. Añade que esta apreciación fue realizada con carácter concluyente por el legislador italiano cuando estableció que la autorización para obtener los datos debía concederse, en particular, para todos los delitos castigados con pena privativa de libertad máxima no inferior a tres años.

24 En estas circunstancias, el Giudice delle indagini preliminari presso il Tribunale di Bolzano (Juez de Instrucción del Tribunal de Bolzano) decidió suspender el procedimiento y plantear al Tribunal de Justicia la siguiente cuestión prejudicial:

«¿Se opone el artículo 15, apartado 1, de la Directiva [2002/58] a la normativa nacional recogida en el artículo 132[, apartado 3,] del Decreto Legislativo [n.º 196/2003], que […] establece:

“3. Dentro del plazo de conservación impuesto por la ley, si existen indicios suficientes de un delito para el que la ley establezca una pena de prisión permanente o una pena máxima de prisión no inferior a 3 años, determinada de conformidad con el artículo 4 del Código de Enjuiciamiento Criminal, y de delitos de amenazas y de acoso u hostigamiento por teléfono contra las personas, si las amenazas, el acoso y el hostigamiento son graves, cuando sea pertinente para la determinación de los hechos, se obtendrán los datos previa autorización del juez mediante auto motivado, a solicitud del Ministerio Fiscal o del abogado del imputado, del investigado, de la víctima y de las otras partes particulares?”»

Sobre la admisibilidad de la petición de decisión prejudicial

25 El Gobierno italiano e Irlanda sostienen que la petición de decisión prejudicial es en parte inadmisible. Señalan que las solicitudes de acceso a los datos conservados por los proveedores de servicios de comunicaciones electrónicas fueron presentadas por el Ministerio Fiscal, sobre la base del artículo 132, apartado 3, del Decreto Legislativo n.º 196/2003, con el fin de perseguir delitos de hurto con circunstancias agravantes de teléfono móvil. Pues bien, a su juicio, mediante su cuestión prejudicial, el órgano jurisdiccional remitente pregunta también al Tribunal de Justicia si el artículo 15, apartado 1, de la Directiva 2002/58 se opone a una disposición nacional que permite obtener el acceso a datos conservados por los proveedores de servicios de comunicaciones electrónicas para perseguir delitos comprendidos en el artículo 132, apartado 3, del Decreto Legislativo n.º 196/2003 distintos de los controvertidos en el litigio principal, como el hurto simple o el acoso grave por teléfono. Por lo tanto, a su juicio, la petición de decisión prejudicial tiene carácter hipotético en la medida en que se refiere a esos otros delitos.

26 A este respecto, es preciso recordar que, según reiterada jurisprudencia, en el marco de la cooperación entre el Tribunal de Justicia y los órganos jurisdiccionales nacionales establecida en el artículo 267 TFUE, corresponde exclusivamente al órgano jurisdiccional nacional que conoce del litigio y que debe asumir la responsabilidad de la decisión jurisdiccional que debe adoptarse apreciar, a la luz de las particularidades del asunto, tanto la necesidad de una decisión prejudicial para poder dictar su sentencia como la pertinencia de las cuestiones que plantea al Tribunal de Justicia. Por consiguiente, cuando las cuestiones planteadas se refieren a la interpretación del Derecho de la Unión, el Tribunal de Justicia está, en principio, obligado a pronunciarse [sentencia de 21 de marzo de 2023, Mercedes-Benz Group (Responsabilidad de los fabricantes de vehículos equipados con dispositivos de desactivación), C-100/21, EU:C:2023:229, apartado 52 y jurisprudencia citada].

27 De ello se sigue que las cuestiones relativas al Derecho de la Unión gozan de una presunción de pertinencia. El Tribunal de Justicia solo puede abstenerse de pronunciarse sobre una cuestión prejudicial planteada por un órgano jurisdiccional nacional cuando resulte evidente que la interpretación del Derecho de la Unión solicitada no guarda relación alguna ni con la realidad ni con el objeto del litigio principal, cuando el problema sea de naturaleza hipotética o cuando el Tribunal de Justicia no disponga de los elementos de hecho y de Derecho necesarios para dar una respuesta útil a las cuestiones que se le hayan planteado [sentencia de 21 de marzo de 2023, Mercedes-Benz Group (Responsabilidad de los fabricantes de vehículos equipados con dispositivos de desactivación), C-100/21, EU:C:2023:229, apartado 53 y jurisprudencia citada].

28 Pues bien, al reproducir íntegramente el artículo 132, apartado 3, del Decreto Legislativo n.º 196/2003, la cuestión prejudicial, aunque no distinga los tipos de delitos a los que se aplica esta disposición, abarca necesariamente los delitos de hurto con circunstancias agravantes respecto de los cuales se han presentado en el litigio principal las solicitudes de autorización de acceso a los datos personales.

29 En consecuencia, esta cuestión no tiene carácter hipotético y, por tanto, es admisible.

Sobre la cuestión prejudicial

30 Como ha señalado el Gobierno francés en sus observaciones escritas, la cuestión planteada por el órgano jurisdiccional remitente, tal como ha sido formulada, insta al Tribunal de Justicia a pronunciarse sobre la compatibilidad del artículo 132, apartado 3, del Decreto Legislativo n.º 196/2003 con el artículo 15, apartado 1, de la Directiva 2002/58.

31 A este respecto, procede recordar que, en el marco del procedimiento establecido en el artículo 267 TFUE, el Tribunal de Justicia no es competente para pronunciarse ni sobre la interpretación de disposiciones legislativas o reglamentarias nacionales ni sobre la conformidad de tales disposiciones con el Derecho de la Unión. En efecto, de reiterada jurisprudencia se desprende que, en el marco de una remisión prejudicial con arreglo al artículo 267 TFUE, el Tribunal de Justicia solo puede interpretar el Derecho de la Unión dentro de los límites de las competencias atribuidas a la Unión [sentencia de 14 de diciembre de 2023, Getin Noble Bank (Plazo de prescripción de las acciones de restitución), C-28/22, EU:C:2023:992, apartado 53 y jurisprudencia citada].

32 Sentado lo anterior, de una jurisprudencia reiterada se desprende que, frente a cuestiones prejudiciales formuladas de manera impropia o sobrepasando el marco de las funciones que le atribuye el artículo 267 TFUE, el Tribunal de Justicia tiene la facultad de extraer, de todos los elementos facilitados por el órgano jurisdiccional nacional y, especialmente, de los fundamentos de Derecho de la resolución de remisión, los elementos del Derecho de la Unión que requieren una interpretación habida cuenta del objeto del litigio. Desde este punto de vista, corresponde al Tribunal de Justicia reformular, en su caso, las cuestiones prejudiciales que se le han planteado (sentencia de 14 de diciembre de 2023, Sparkasse Südpfalz, C-206/22, EU:C:2023:984, apartado 20 y jurisprudencia citada).

33 Además, el Tribunal de Justicia puede verse obligado a tomar en consideración normas del Derecho de la Unión a las que el juez nacional no se haya referido en el enunciado de su cuestión (sentencia de 17 de noviembre de 2022, Harman International Industries, C-175/21, EU:C:2022:895, apartado 31 y jurisprudencia citada).

34 Habida cuenta de lo anterior, procede considerar que, 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 una disposición nacional que obliga al juez nacional, que interviene en el marco de un control previo efectuado a raíz de una solicitud motivada de acceso a un conjunto de datos de tráfico o de localización, que pueden permitir que se extraigan conclusiones precisas sobre la vida privada de un usuario de un medio de comunicación electrónica, conservados por los proveedores de servicios de comunicaciones electrónicas, presentada por una autoridad nacional competente en el marco de una investigación penal, a autorizar dicho acceso si se solicita con el fin de investigar delitos castigados, por el Derecho nacional, con una pena máxima de privación de libertad no inferior a tres años, siempre que existan indicios suficientes de tales delitos y que dichos datos sean pertinentes para constatar los hechos.

35 Con carácter preliminar, procede recordar que, por lo que respecta a las condiciones en las que puede concederse a las autoridades públicas acceso a los datos de tráfico y de localización conservados por los proveedores de servicios de comunicaciones electrónicas, con fines de prevención, investigación, descubrimiento y persecución de delitos con arreglo a una medida legislativa adoptada en virtud del artículo 15, apartado 1, de la Directiva 2002/58, el Tribunal de Justicia ha declarado que tal acceso solo puede concederse en la medida en que esos datos hayan sido conservados por dichos proveedores de conformidad con dicha Directiva [véase, en este sentido, la sentencia de hoy, La Quadrature du Net y otros (Datos personales y lucha contra la falsificación), C-470/21, apartado 65 y jurisprudencia citada]. El Tribunal de Justicia también ha señalado que ese 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 [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 30 y jurisprudencia citada].

36 Asimismo, procede recordar la jurisprudencia del Tribunal de Justicia según la cual solo los objetivos de lucha contra la delincuencia grave o de prevención de las amenazas graves contra la seguridad pública pueden justificar la injerencia grave en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta, que deriva del 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, 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 [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 35 y jurisprudencia citada].

37 Mediante su cuestión prejudicial, el órgano jurisdiccional remitente desea saber, en esencia, si puede autorizarse tal injerencia, de carácter grave, para delitos como los contemplados por la normativa nacional controvertida en el litigio principal.

38 Por lo que respecta, de entrada, a si los accesos como los controvertidos pueden calificarse de injerencia grave en los derechos fundamentales garantizados en los artículos 7 y 8 de la Carta, procede señalar que, para identificar a los presuntos autores de los hurtos que dieron lugar a ese litigio, el Ministerio Fiscal, respecto de cada uno de los teléfonos móviles de que se trata, solicitó al órgano jurisdiccional remitente, sobre la base del artículo 132, apartado 3, del Decreto Legislativo n.º 196/2003, autorización para recabar todos los datos en posesión de las compañías telefónicas, obtenidos mediante un método de rastreo y localización de las conversaciones y comunicaciones telefónicas y de las conexiones efectuadas con dichos teléfonos. Estas solicitudes se referían, más concretamente, a los abonados y a los códigos IMEI de los aparatos destinatarios o emisores de llamadas, a los sitios visitados y a los que se accedía, al momento y la duración de las llamadas y conexiones, a la indicación de las partes de redes o repetidores de que se trataba, así como a los abonados y a los códigos IMEI de los aparatos emisores y destinatarios de los SMS o MMS.

39 El acceso a un conjunto de datos de tráfico o de localización de ese tipo parece poder permitir extraer conclusiones 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 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 36 y jurisprudencia citada]. Por lo tanto, la injerencia en los derechos fundamentales garantizados en los artículos 7 y 8 de la Carta causada por el acceso a tales datos puede calificarse de grave.

40 Como se desprende del apartado 39 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), esta apreciación no puede descartarse por el mero hecho de que ambas solicitudes de acceso a los datos de tráfico o de localización en cuestión solo se refirieran a períodos cortos, de menos de dos meses, que iban desde las fechas de los presuntos hurtos de los teléfonos móviles hasta las fechas en las que se redactaron tales solicitudes, ya que esas solicitudes se referían a un conjunto de datos que podía proporcionar información precisa sobre la vida privada de las personas que utilizaban los teléfonos móviles en cuestión.

41 Asimismo, a efectos de apreciar la existencia de una injerencia grave en los derechos garantizados en los artículos 7 y 8 de la Carta, carece de pertinencia el hecho de que los datos a los que el Ministerio Fiscal solicitó acceso no fueran los de los propietarios de los teléfonos móviles en cuestión, sino los de las personas que se hubieran comunicado entre sí utilizando dichos teléfonos después de sus presuntos hurtos. En efecto, del artículo 5, apartado 1, de la Directiva 2002/58 se desprende que la obligación de principio de garantizar la confidencialidad de las comunicaciones electrónicas, y la confidencialidad 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, se refiere a las comunicaciones realizadas por los usuarios de dicha red. Pues bien, el artículo 2, letra a), de esta Directiva define el concepto de «usuario» como la 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.

42 Por consiguiente, habida cuenta de la jurisprudencia citada en el apartado 36 de la presente sentencia, dado que las injerencias en los derechos fundamentales causadas por el acceso a los datos, como las controvertidas en el litigio principal, pueden considerarse graves, solo resulta posible justificarlas por los objetivos de lucha contra la delincuencia grave o de prevención de amenazas graves para la seguridad pública.

43 A continuación, si bien 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, una normativa de este tipo debe establecer reglas claras y precisas que regulen el alcance y los requisitos de aplicación de tal acceso. 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 puedan estar implicadas en un delito grave. Para garantizar en la práctica el íntegro cumplimiento de estos requisitos, garantizando así que la injerencia se limite a lo estrictamente necesario, es esencial que el acceso de las autoridades nacionales competentes a los datos conservados se supedite, salvo en caso de urgencia debidamente justificada, a un control previo efectuado bien por

un órgano jurisdiccional, bien por una entidad administrativa independiente [véase, en ese 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, apartados 48 a 51].

44 Por último, en lo que respecta a la definición del concepto de «delito grave», de la jurisprudencia se desprende que, en la medida en que la Unión no haya legislado en la materia, la legislación penal y las normas de procedimiento penal son competencia de los Estados miembros. No obstante, estos deben ejercer esta competencia respetando el Derecho de la Unión (véase, en este sentido, la sentencia de 26 de febrero de 2019, Rimšēvičs y BCE/Letonia, C-202/18 y C-238/18, EU:C:2019:139, apartado 57 y jurisprudencia citada).

45 A este respecto, procede señalar que la definición de las infracciones penales, de las circunstancias atenuantes y agravantes y de las sanciones refleja tanto la realidad social como las tradiciones jurídicas, que varían no solo entre los Estados miembros, sino también en el tiempo. Pues bien, estas realidades y tradiciones revisten una importancia indudable para determinar qué delitos se consideran graves.

46 Por lo tanto, habida cuenta del reparto de competencias entre la Unión y los Estados miembros en virtud del Tratado FUE y de las importantes diferencias que existen entre los sistemas jurídicos de los Estados miembros en el ámbito penal, procede considerar que corresponde a los Estados miembros definir los «delitos graves» a efectos de la aplicación del artículo 15, apartado 1, de la Directiva 2002/58.

47 No obstante, la definición de «delitos graves» realizada por los Estados miembros debe respetar las exigencias que se derivan de dicho artículo 15, apartado 1, interpretado a la luz de los artículos 7, 8, 11 y 52, apartado 1, de la Carta.

48 A este respecto, procede recordar que en la medida en que permite a los Estados miembros adoptar medidas legales para «limitar el alcance» de los derechos y obligaciones que se establecen en particular en los artículos 5, 6 y 9 de la Directiva 2002/58, como los derivados de los principios de confidencialidad de las comunicaciones y de prohibición de almacenamiento de los datos asociados a ellas, el artículo 15, apartado 1, de esa Directiva introduce una excepción a la regla general establecida, en particular, en dichos artículos 5, 6 y 9, por lo que, conforme a reiterada jurisprudencia, debe ser objeto de una interpretación estricta. En consecuencia, tal disposición 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 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).

49 Además, del artículo 15, apartado 1, tercera frase, de la Directiva 2002/58 se infiere que las medidas adoptadas por los Estados miembros con arreglo a esta disposición deben respetar los principios generales del Derecho de la Unión, entre los que figura el principio de proporcionalidad, y los derechos fundamentales garantizados por los artículos 7, 8 y 11 de la Carta (véase, en ese sentido, la sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 42).

50 De ello se deduce que los Estados miembros no pueden desnaturalizar el concepto de «delito grave» y, por extensión, el de «delincuencia grave», incluyendo en él, a efectos de la aplicación de dicho artículo 15, apartado 1, delitos que manifiestamente no son graves, habida cuenta de las condiciones sociales en el Estado miembro de que se trate, pese a que el legislador de dicho Estado miembro ha previsto castigarlos con una pena privativa de libertad máxima de tres años.

51 Para comprobar en particular la inexistencia de tal desnaturalización es esencial que, cuando el acceso de las autoridades nacionales competentes a los datos conservados implique el riesgo de una injerencia grave en los derechos fundamentales del interesado, dicho acceso esté supeditado a un control previo efectuado bien por un órgano jurisdiccional, bien por una entidad administrativa independiente [véase, en este sentido, la sentencia de hoy, La Quadrature du Net y otros (Datos personales y lucha contra la falsificación), C-470/21, apartados 124 a 131].

52 En el caso de autos, de la resolución de remisión se desprende que el artículo 132, apartado 3, del Decreto Legislativo n.º 196/2003 establece los requisitos con arreglo a los cuales el acceso a los datos conservados por los proveedores de servicios de comunicaciones electrónicas puede ser concedido por un juez que conoce de una solicitud motivada de una autoridad pública. Esta

disposición define los delitos para cuyo enjuiciamiento puede concederse el acceso a los datos conservados por los proveedores de servicios de comunicaciones electrónicas, con referencia a una pena privativa de libertad máxima no inferior a tres años, y supedita dicho acceso al doble requisito de que existan «indicios suficientes de un delito» y de que dichos datos sean «pertinentes para la determinación de los hechos».

53 No obstante, el órgano jurisdiccional remitente se pregunta si la definición, resultante de esta disposición, de los «delitos graves», para cuyo enjuiciamiento puede concederse el acceso a los datos, no es demasiado amplia, puesto que abarca delitos que únicamente causan una alarma social limitada.

54 A este respecto, procede señalar, en primer lugar, que una definición según la cual los «delitos graves», para cuyo enjuiciamiento puede concederse el acceso, son aquellos castigados con una pena máxima privativa de libertad al menos igual a una duración que la ley determina, se basa en un criterio objetivo. Ello es conforme con la exigencia de que 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 (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 105 y jurisprudencia citada).

55 En segundo lugar, de la jurisprudencia citada en el apartado 48 de la presente sentencia se desprende que la definición dada en Derecho nacional de los «delitos graves» que pueden permitir el acceso a los datos conservados por los proveedores de servicios de comunicaciones electrónicas, que permiten extraer conclusiones precisas sobre la vida privada de los interesados, no debe ser tan amplia que el acceso a esos datos se convierta en la regla más que en la excepción. Así pues, no podría abarcar la gran mayoría de los delitos, lo que sucedería si el umbral más allá del cual la pena máxima privativa de libertad con que se castiga un delito justifica que este se califique de delito grave se fija en un nivel excesivamente bajo.

56 Pues bien, un umbral fijado por referencia a una pena privativa de libertad máxima de tres años no parece, a este respecto, excesivamente bajo (véase, en este sentido, la sentencia de 21 de junio de 2022, Ligue des droits humains, C-817/19, EU:C:2022:491, apartado 150).

57 Ciertamente, dado que la definición de «delitos graves», para los que puede solicitarse el acceso a los datos conservados por los proveedores de comunicaciones electrónicas, se establece por referencia no a la pena mínima aplicable, sino a la pena máxima aplicable, no debe excluirse que el acceso a los datos, constitutivo de una injerencia grave en los derechos fundamentales, pueda solicitarse con fines de enjuiciamiento de delitos que, en realidad, no constituyen delitos graves (véase, por analogía, la sentencia de 21 de junio de 2022, Ligue des droits humains, C-817/19, EU:C:2022:491, apartado 151).

58 Sin embargo, la fijación de un umbral a partir del cual la pena privativa de libertad máxima con que se castiga un delito justifica que este se califique de delito grave no es necesariamente contraria al principio de proporcionalidad.

59 Por una parte, tal parece ser el caso de una disposición como la controvertida en el litigio principal, puesto que, como se desprende de la resolución de remisión, tiene por objeto, con carácter general, el acceso a los datos conservados por los proveedores de servicios de comunicaciones electrónicas, sin precisar la naturaleza de esos datos. Así pues, esta disposición parece abarcar, en particular, los casos en los que el acceso no puede calificarse de injerencia grave, ya que no se refiere a un conjunto de datos que permita extraer conclusiones precisas sobre la vida privada de las personas afectadas.

60 Por otra parte, el órgano jurisdiccional o el organismo administrativo independiente, que interviene en el marco de un control previo efectuado a raíz de una solicitud motivada de acceso, debe estar facultado para denegar o restringir dicho acceso si constata que la injerencia en los derechos fundamentales que constituiría tal acceso es grave cuando resulte evidente que el delito en cuestión no forma parte efectivamente de la delincuencia grave (véase, por analogía, la sentencia de 21 de junio de 2022, Ligue des Derechos Humanos, C-817/19, EU:C:2022:491, apartado 152).

61 En efecto, el órgano jurisdiccional o la entidad encargada del control debe poder garantizar un justo equilibrio entre, por un lado, los intereses legítimos vinculados a las necesidades de la investigación en el marco de la lucha contra la delincuencia y, por otro lado, los derechos fundamentales al respeto de la vida privada y a la protección de los datos personales de las

personas cuyos datos se ven afectados por el acceso [sentencia de hoy, La Quadrature du Net y otros (Datos personales y lucha contra la falsificación), C-470/21, apartado 125 y jurisprudencia citada].

62 En particular, en el marco de su examen de la proporcionalidad de la injerencia causada en los derechos fundamentales de la persona afectada por la solicitud de acceso, dicho órgano jurisdiccional o dicha entidad debe poder excluir tal acceso cuando este se solicita en el marco de un proceso por un delito que manifiestamente no es grave, en el sentido del apartado 50 de la presente sentencia.

63 De lo anterior resulta que 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 no se opone a una disposición nacional que obliga al juez nacional, que interviene en el marco de un control previo efectuado a raíz de una solicitud motivada de acceso a un conjunto de datos de tráfico o de localización, que pueden permitir que se extraigan conclusiones precisas sobre la vida privada de un usuario de un medio de comunicación electrónica, conservados por los proveedores de servicios de comunicaciones electrónicas, presentada por una autoridad nacional competente en el marco de una investigación penal, a autorizar dicho acceso si se solicita con el fin de investigar delitos castigados, por el Derecho nacional, con una pena máxima de privación de libertad no inferior a tres años, siempre que existan indicios suficientes de tales delitos y que dichos datos sean pertinentes para constatar los hechos, y a condición, no obstante, de que ese juez esté facultado para denegar tal acceso si se solicita en el marco de una investigación sobre un delito que manifiestamente no sea grave, habida cuenta de las condiciones sociales en el Estado miembro de que se trate.

Costas

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

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

El artículo 15, apartado 1, de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), en su versión modificada por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, 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

no se opone a una disposición nacional que obliga al juez nacional, que interviene en el marco de un control previo efectuado a raíz de una solicitud motivada de acceso a un conjunto de datos de tráfico o de localización, que pueden permitir que se extraigan conclusiones precisas sobre la vida privada de un usuario de un medio de comunicación electrónica, conservados por los proveedores de servicios de comunicaciones electrónicas, presentada por una autoridad nacional competente en el marco de una investigación penal, a autorizar dicho acceso si se solicita con el fin de investigar delitos castigados, por el Derecho nacional, con una pena máxima de privación de libertad no inferior a tres años, siempre que existan indicios suficientes de tales delitos y que dichos datos sean pertinentes para constatar los hechos, y a condición, no obstante, de que ese juez esté facultado para denegar tal acceso si se solicita en el marco de una investigación sobre un delito que manifiestamente no sea grave, habida cuenta de las condiciones sociales en el Estado miembro de que se trate.

Firmas