Edición provisional

SENTENCIA DEL TRIBUNAL DE JUSTICIA (Gran Sala)

de 20 de septiembre de 2022 (*)

«Procedimiento prejudicial — Tratamiento de datos de carácter personal en el sector de las comunicaciones electrónicas — Confidencialidad de las comunicaciones — Proveedores de servicios de comunicaciones electrónicas — Conservación generalizada e indiferenciada de los datos de tráfico y de localización — Directiva 2002/58/CE — Artículo 15, apartado 1 — Carta de los Derechos Fundamentales de la Unión Europea — Artículos 6, 7, 8 y 11 y artículo 52, apartado 1 — Artículo 4 TUE, apartado 2»

En los asuntos acumulados C-793/19 y C-794/19,

que tienen por objeto sendas peticiones de decisión prejudicial planteadas, con arreglo al artículo 267 TFUE, por el Bundesverwaltungsgericht (Tribunal Supremo de lo Contencioso-Administrativo, Alemania), mediante resoluciones de 25 de septiembre de 2019, recibidas en el Tribunal de Justicia el 29 de octubre de 2019, en los procedimientos entre

Bundesrepublik Deutschland, representada por la Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen,

y

SpaceNet AG (asunto C-793/19),

Telekom Deutschland GmbH (asunto C-794/19),

EL TRIBUNAL DE JUSTICIA (Gran Sala),

integrado por el Sr. K. Lenaerts, Presidente, el Sr. A. Arabadjiev, la Sra. A. Prechal, los Sres. S. Rodin e I. Jarukaitis y la Sra. I. Ziemele, Presidentes de Sala, y los Sres. T. von Danwitz, M. Safjan, F. Biltgen, P. G. Xuereb (Ponente) y N. Piçarra, la Sra. L. S. Rossi y por el Sr. A. Kumin, Jueces;

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

Secretario: Sr. D. Dittert, jefe de unidad;

habiendo considerado los escritos obrantes en autos y celebrada la vista el 13 de septiembre de 2021;

consideradas las observaciones presentadas:

– en nombre de la Bundesrepublik Deutschland, representada por la Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, por el Sr. C. Mögelin, en calidad de agente;

– en nombre de SpaceNet AG, por el Sr. M. Bäcker, Rechtsanwalt;

– en nombre de Telekom Deutschland GmbH, por el Sr. T. Mayen, Rechtsanwalt;

– en nombre del Gobierno alemán, por los Sres. J. Möller, F. Halibi, M. Hellmann, D. Klebs y E. Lankenau, en calidad de agentes;

– en nombre del Gobierno danés, por los Sres. M. Jespersen, J. Nymann-Lindegren y por las Sras. V. Pasternak Jørgensen y M. Søndahl Wolff, en calidad de agentes;

– en nombre del Gobierno estonio, por las Sras. A. Kalbus y M. Kriisa, en calidad de agentes;

– en nombre de Irlanda, por el Sr. A. Joyce y por la Sra. J. Quaney, en calidad de agentes, asistidos por los Sres. D. Fennelly, BL, y P. Gallagher, SC;

– en nombre del Gobierno español, por el Sr. L. Aguilera Ruiz, en calidad de agente;

– en nombre del Gobierno francés, por la Sra. A. Daniel, los Sres. D. Dubois y J. Illouz, la Sra. E. de Moustier y por el Sr. T. Stéhelin, en calidad de agentes;

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

– en nombre del Gobierno neerlandés, por las Sras. M. K. Bulterman, A. Hanje y C. S. Schillemans, en calidad de agentes;

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

– en nombre del Gobierno finlandés, por las Sras. A. Laine y M. Pere, en calidad de agentes;

– en nombre del Gobierno sueco, por las Sras. H. Eklinder, A. Falk, J. Lundberg, C. Meyer-Seitz, R. Shahsavan Eriksson y H. Shev, en calidad de agentes;

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

– en nombre del Supervisor Europeo de Protección de Datos, por la Sra. A. Buchta y por los Sres. D. Nardi, N. Stolič y K. Ujazdowski, en calidad de agentes;

oídas las conclusiones del Abogado General, presentadas en audiencia pública el 18 de noviembre de 2021;

dicta la siguiente

Sentencia

1 Las peticiones de decisión prejudicial tienen 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 6 a 8 y 11 y el artículo 52, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, «Carta») y con el artículo 4 TUE, apartado 2.

2 Estas peticiones se han presentado en el contexto de sendos litigios entre la Bundesrepublik Deutschland (República Federal de Alemania), representada por la Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (Agencia Federal de las Redes de Electricidad, Gas, Telecomunicaciones, Correos y Ferrocarriles, Alemania), y SpaceNet AG (asunto C-793/19) y Telekom Deutschland GmbH (asunto C-794/19) en relación con la obligación impuesta a estas últimas de conservar datos de tráfico y de localización relativos a las telecomunicaciones de sus clientes.

Marco jurídico

Derecho de la Unión

Directiva 95/46/CE

3 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), fue derogada, con efectos a partir del 25 de mayo de 2018, por el 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 (Reglamento general de protección de datos) (DO 2016, L 119, p. 1).

4 El artículo 3, apartado 2, de la Directiva 95/46 establecía que:

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

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

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

Directiva 2002/58

5 Los considerandos 2, 6, 7 y 11 de la Directiva 2002/58 exponen:

«(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].

[…]

(6) Internet está revolucionando las estructuras tradicionales del mercado al aportar una infraestructura común mundial para la prestación de una amplia gama de servicios de comunicaciones electrónicas. Los servicios de comunicaciones electrónicas disponibles al público a través de Internet introducen nuevas posibilidades para los usuarios, pero también nuevos riesgos para sus datos personales y su intimidad.

(7) En el caso de las redes públicas de comunicación, deben elaborarse disposiciones legales, reglamentarias y técnicas específicas con objeto de proteger los derechos y libertades fundamentales de las personas físicas y los intereses legítimos de las personas jurídicas, en particular frente a la creciente capacidad de almacenamiento y tratamiento informático de datos relativos a abonados y usuarios.

[…]

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

6 El artículo 1 de esta Directiva, titulado «Ámbito de aplicación y objetivo», dispone:

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

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

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

7 A tenor del artículo 2 de dicha 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;

[…]».

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

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

9 A tenor del artículo 5 de esta Directiva, 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.»

10 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 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.

[…]»

11 El artículo 9 de esta Directiva, 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. […]»

12 El artículo 15 de la Directiva 2002/58, titulado «Aplicación de determinadas disposiciones de la Directiva [95/46]», dispone en su apartado 1:

«Los Estados miembros podrán adoptar medidas legales para limitar el alcance de los derechos y las obligaciones que se establecen en los artículos 5 y 6, en los apartados 1 a 4 del artículo 8 y en el artículo 9 de la presente Directiva, cuando tal limitación constituya una medida necesaria proporcionada y apropiada en una sociedad democrática para proteger la seguridad nacional (es decir, la seguridad del Estado), la defensa, la seguridad pública, o la prevención, investigación, descubrimiento y persecución de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas a que se hace referencia en el apartado 1 del artículo 13 de la Directiva [95/46]. 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 alemán

TKG

13 El artículo 113a, apartado 1, primera frase, de la Telekommunikationsgesetz (Ley de Telecomunicaciones), de 22 de junio de 2004 (BGBl. 2004 I, p. 1190), en su versión aplicable al litigio principal (en lo sucesivo, «TKG»), tiene el siguiente tenor:

«Las obligaciones relativas a la conservación, utilización y seguridad de los datos de tráfico definidas en los artículos 113b a 113g se refieren a los operadores que proveen a los usuarios finales servicios de telecomunicación accesibles al público.»

14 En virtud del artículo 113b de la TKG:

«(1) Los operadores a los que se refiere el artículo 113a, apartado 1, deben conservar los datos en el territorio nacional de la siguiente manera:

1. durante diez semanas si se trata de los datos a los que se refieren los apartados 2 y 3,

2. durante cuatro semanas si se trata de los datos de localización a los que se refiere el apartado 4.

(2) Los proveedores de servicios telefónicos accesibles al público conservarán

1. el número de llamada u otra identificación de las líneas de origen y de destino, así como de cualquier otra línea utilizada en caso de redirección o de desvío de llamada,

2. la fecha y la hora del inicio y el fin de la comunicación, con indicación de la zona horaria,

3. las indicaciones relativas al servicio utilizado cuando puedan utilizarse servicios diferentes en el marco del servicio telefónico,

4. además, en el caso de servicios de telefonía móvil,

   a) la identificación internacional del usuario móvil de la línea de origen y de destino,

   b) la identificación internacional de las terminales de origen y de destino,

c) la fecha y la hora de la primera activación del servicio, con indicación de la zona horaria si se trata de servicios de pago anticipado,

5. así como, en el caso de los servicios de telefonía por Internet, las direcciones IP (protocolo de Internet) de la línea de origen y de destino y los números de identificación asignados.

El primer párrafo se aplicará *mutatis mutandis*

1. en caso de comunicación por SMS, mensaje multimedia o similar; en este caso, las indicaciones referidas en el párrafo primero, punto 2, se sustituyen por el momento del envío y de la recepción del mensaje;

2. a las llamadas sin respuesta o infructuosas en razón de una intervención del gestor de la red […]

(3) Los proveedores de servicios de acceso a Internet accesibles al público conservarán

1. la dirección IP asignada al abonado a los fines de la utilización de Internet,

2. la identificación clara de la conexión que permite el acceso a Internet, así como el número de identificación atribuido,

3. la fecha y hora de inicio y fin del uso de Internet con la dirección de protocolo de Internet asignada, con indicación de la zona horaria;

(4) En caso de utilización de servicios de telefonía móvil, habrá de conservarse la designación de las células telefónicas utilizadas al inicio de la comunicación por quien hace la llamada y por quien la recibe. Por lo que hace a los servicios de acceso a Internet accesibles al público, habrá de conservarse, en caso de utilización móvil, la designación de las células telefónicas utilizadas al inicio de la conexión a Internet. Conviene igualmente conservar los datos que permiten conocer la posición geográfica y las direcciones de radiación máxima de las antenas que sirven a la célula telefónica concernida.

(5) El contenido de la comunicación, los datos relativos a los sitios Internet consultados y los datos de los servicios de correo electrónico no pueden ser conservados en virtud de la presente disposición.

(6) Los datos subyacentes a las comunicaciones contempladas en el artículo 99, apartado 2, no pueden ser conservados en virtud de la presente disposición. Esto se aplica, *mutatis mutandis*, a las comunicaciones telefónicas procedentes de las entidades contempladas en el artículo 99, apartado 2. El artículo 99, apartado 2, frases segunda a séptima, se aplica *mutatis mutandis*.

[…]»

15 Las comunicaciones a que se refiere el artículo 99, apartado 2, de la TKG, a las que se remite el artículo 113b, apartado 6, de la TKG, son comunicaciones con personas, autoridades y organizaciones de carácter social o religioso que ofrecen única o esencialmente a interlocutores, en principio anónimos, servicios de asistencia telefónica en casos de situaciones de urgencia psicológica o social y que están sujetas, ellas mismas o sus colaboradores, a obligaciones de confidencialidad particulares a este respecto. La excepción prevista en el artículo 99, apartado 2, frases segunda y cuarta, de la TKG está supeditada a la inclusión de receptores de las llamadas, a petición suya, en una lista elaborada por la Agencia Federal de las Redes de Electricidad, Gas, Telecomunicaciones, Correos y Ferrocarriles, después de que los titulares de los números de llamada hayan acreditado su misión mediante la presentación de una certificación expedida por una autoridad, organismo, establecimiento o fundación de Derecho público.

16 A tenor del artículo 113c, apartados 1 y 2, de la TKG:

«(1) Los datos conservados en virtud del artículo 113b pueden

1. ser transmitidos a una autoridad represiva cuanto esta solicite la transmisión invocando una disposición legal que la autorice a reunir los datos contemplados en el artículo 113b a los fines de

la represión de infracciones penales particularmente graves;

2. ser transmitidos a una autoridad de seguridad de los *Länder* cuando esta solicite la transmisión invocando una disposición legal que la autorice a reunir los datos contemplados en el artículo 113b a los fines de la prevención de un riesgo concreto para la integridad física, la vida o la libertad de una persona o bien para la existencia del Estado federal o del *Land*;

[…]

(2) Los datos conservados en virtud del artículo 113b no pueden ser utilizados, por quienes están sujetos a las obligaciones establecidas en el artículo 113a, apartado 1, a otros fines que no sean los contemplados en el apartado 1.»

17 El artículo 113d de la TKG establece:

«El destinatario de la obligación prevista en el artículo 113a, apartado 1, debe velar por que los datos conservados de conformidad con el artículo 113b, apartado 1, en virtud de la obligación de conservación estén protegidos, por medidas técnicas y de organización conformes al estado de la técnica, contra el control y la utilización no autorizados. Estas medidas comprenden en particular:

1. la utilización de un procedimiento de encriptación particularmente seguro,

2. el almacenamiento en infraestructuras de almacenamiento distintas, separadas de las afectas a funciones operacionales corrientes,

3. el almacenamiento, dotado de un nivel de protección elevado contra los ciberataques, en sistemas informáticos de tratamiento de datos desconectados,

4. la restricción del acceso a las instalaciones utilizadas para el tratamiento de datos a las personas que dispongan de una habilitación especial conferida por el responsable de la obligación y

5. la obligación de hacer intervenir, durante el acceso a los datos, al menos a dos personas que dispongan de una habilitación especial conferida por el responsable de la obligación.»

18 El artículo 113e de la TKG establece:

«(1) El responsable de la obligación prevista en el artículo 113a, apartado 1, debe velar por que, a los fines del control de la protección de datos, se consigne cada acceso, y en particular la lectura, la copia, la modificación, la eliminación y el cierre, a los datos conservados de conformidad con el artículo 113b, apartado 1, en virtud de la obligación de conservación. Deben consignarse

1. la hora del acceso,

2. las personas que acceden a los datos,

3. el objeto y la naturaleza del acceso.

(2) Los datos consignados no pueden ser utilizados a otros fines que los del control de la protección de los datos.

(3) El responsable de la obligación prevista en el artículo 113a, apartado 1, debe velar por que los datos consignados se eliminen al cabo de un año.»

19 Con el fin de garantizar un nivel de seguridad y de calidad de los datos particularmente elevado, la Agencia Federal de las Redes de Electricidad, Gas, Telecomunicaciones, Correos y Ferrocarriles establece, con arreglo al artículo 113f, apartado 1, de la TKG, un conjunto de exigencias que, en virtud del artículo 113f, apartado 2, de esta, deben ser evaluadas de forma permanente y, en su caso, adaptadas. El artículo 113g de la TKG exige que se integren medidas de seguridad específicas en la exposición de la política en materia de seguridad que debe presentar el responsable de la obligación.

StPO

20 El artículo 100g, apartado 2, primera frase, de la Strafprozessordnung (Ley de Enjuiciamiento Criminal; en lo sucesivo, «StPO») tiene el siguiente tenor:

«Si determinados hechos permiten sospechar que alguien ha cometido, en calidad de autor o de cómplice, una de las infracciones penales particularmente graves contempladas en la segunda frase o, en los casos en los que la tentativa de una infracción es punible, ha intentado cometerla y si la infracción es también particularmente grave en el caso concreto, los datos relativos al tráfico, conservados de conformidad con el artículo 113b de la [TKG], pueden ser recogidos en el caso de que la investigación sobre los hechos o la localización de la persona investigada sean excesivamente difíciles o inviables por otros medios y si la recolección de los datos es proporcional a la importancia del asunto.»

21 El artículo 101a, apartado 1, de la StPO somete a autorización judicial la recolección de datos relativos al tráfico con arreglo al artículo 100g de la StPO. En virtud del artículo 101a, apartado 2, de esa misma Ley, la decisión judicial debe contener las consideraciones esenciales relativas al carácter necesario y pertinente de la medida en el caso concreto. El artículo 101a, apartado 6, de la StPO establece la obligación de informar a los participantes en la telecomunicación de que se trate.

Litigios principales y cuestión prejudicial

22 SpaceNet y Telekom Deutschland prestan, en Alemania, servicios de acceso a Internet disponibles al público. La segunda presta, además, también en Alemania, servicios telefónicos disponibles al público.

23 Estos prestadores de servicios impugnaron ante el Verwaltungsgericht Köln (Tribunal de lo Contencioso-Administrativo de Colonia, Alemania) la obligación que les impone el artículo 113a, apartado 1, en relación con el artículo 113b de la TKG, de conservar datos de tráfico y datos de localización relativos a las telecomunicaciones de sus clientes a partir del 1 de julio de 2017.

24 Mediante sentencias de 20 de abril de 2018, el Verwaltungsgericht Köln (Tribunal de lo Contencioso-Administrativo de Colonia) declaró que SpaceNet y Telekom Deutschland no estaban obligadas a conservar los datos de tráfico relativos a las telecomunicaciones mencionados en el artículo 113b, apartado 3, de la TKG de los clientes a los que proporcionan acceso a Internet y que, además, Telekom Deutschland no estaba obligada a conservar los datos de tráfico relativos a las telecomunicaciones mencionados en el artículo 113b, apartado 2, frases primera y segunda, de la TKG de los clientes a los que presta acceso a servicios de telefonía disponibles al público. En efecto, dicho órgano jurisdiccional consideró, a la luz de la sentencia de 21 de diciembre de 2016, Tele2 Sverige y Watson y otros (C-203/15 y C-698/15, EU:C:2016:970), que esta obligación de conservación era contraria al Derecho de la Unión.

25 La República Federal de Alemania interpuso sendos recursos de casación contra estas sentencias ante el Bundesverwaltungsgericht (Tribunal Supremo de lo Contencioso-Administrativo, Alemania), que es el órgano jurisdiccional remitente.

26 Este considera que la cuestión de si la obligación de conservación impuesta por las disposiciones del artículo 113a, apartado 1, en relación con el artículo 113b de la TKG, es contraria al Derecho de la Unión depende de la interpretación de la Directiva 2002/58.

27 A este respecto, el órgano jurisdiccional remitente señala que el Tribunal de Justicia ya ha declarado con carácter definitivo, en la sentencia de 21 de diciembre de 2016, Tele2 Sverige y Watson y otros (C-203/15 y C-698/15, EU:C:2016:970), que las normativas relativas a la conservación de los datos de tráfico y de localización, así como al acceso a esos datos por las autoridades nacionales, están comprendidas, en principio, en el ámbito de aplicación de la Directiva 2002/58.

28 Asimismo, señala que la obligación de conservación controvertida en los litigios principales, en la medida en que limita los derechos derivados de los artículos 5, apartado 1, 6, apartado 1, y 9, apartado

1, de la Directiva 2002/58, solo puede justificarse sobre la base del artículo 15, apartado 1, de dicha Directiva.

29 A este respecto, recuerda que de la sentencia de 21 de diciembre de 2016, Tele2 Sverige y Watson y otros (C-203/15 y C-698/15, EU:C:2016:970), se desprende que el artículo 15, apartado 1, de la Directiva 2002/58, interpretado a la luz de los artículos 7, 8 y 11 y del artículo 52, apartado 1, de la Carta, debe interpretarse en el sentido de que se opone a una normativa nacional que establece, con el fin de luchar contra la delincuencia, una conservación generalizada e indiferenciada de todos los datos de tráfico y de localización de todos los abonados y usuarios registrados en relación con todos los medios de comunicación electrónica.

30 Pues bien, según el órgano jurisdiccional remitente, al igual que las normativas nacionales controvertidas en los asuntos que dieron lugar a dicha sentencia, la normativa nacional controvertida en los litigios principales no exige ningún motivo para la conservación de los datos ni ninguna relación entre los datos conservados y una infracción penal o un riesgo para la seguridad pública. Según explica, dicha normativa nacional prescribe la conservación, sin ningún motivo, generalizada y sin distinción personal, temporal o geográfica, de la mayor parte de los datos pertinentes de tráfico relacionados con telecomunicaciones.

31 No obstante, el órgano jurisdiccional remitente considera que no cabe excluir que la obligación de conservación controvertida en los litigios principales pueda estar justificada en virtud del artículo 15, apartado 1, de la Directiva 2002/58.

32 En primer lugar, señala que, a diferencia de las normativas nacionales controvertidas en los asuntos que dieron lugar a la sentencia de 21 de diciembre de 2016, Tele2 Sverige y Watson y otros (C-203/15 y C-698/15, EU:C:2016:970), la normativa nacional controvertida en los litigios principales no exige la conservación de todos los datos de tráfico relativos a las telecomunicaciones de todos los abonados y usuarios registrados en lo que respecta a todos los medios de comunicación electrónica. Indica que no solo el contenido de las comunicaciones queda excluido de la obligación de conservación, sino que los datos relativos a los sitios de Internet consultados, los datos de los servicios de correo electrónico y los datos en los que se basan las comunicaciones de carácter social o religioso hacia o a partir de determinadas líneas no pueden conservarse, como se desprende del artículo 113b, apartados 5 y 6, de la TKG.

33 En segundo lugar, dicho órgano jurisdiccional indica que el artículo 113b, apartado 1, de la TKG establece un período de conservación de cuatro semanas para los datos de localización y de diez semanas para los datos de tráfico, mientras que la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE (DO 2006, L 105, p. 54), en la que se basaban las normativas nacionales controvertidas en los asuntos que dieron lugar a la sentencia de 21 de diciembre de 2016, Tele2 Sverige y Watson y otros (C-203/15 y C-698/15, EU:C:2016:970), establecía un período de conservación de entre seis meses y dos años.

34 Pues bien, según el órgano jurisdiccional remitente, si bien la exclusión de determinados medios de comunicación o de determinadas categorías de datos y la limitación del período de conservación no bastan para eliminar el riesgo de que se pueda dibujar un perfil completo de las personas afectadas, este riesgo se reduce cuando menos considerablemente en el marco de la aplicación de la normativa nacional controvertida en los litigios principales.

35 En tercer lugar, el órgano jurisdiccional remitente señala que dicha normativa establece limitaciones estrictas en lo que respecta a la protección de los datos conservados y al acceso a ellos. Así, por un lado, garantiza una protección eficaz de los datos conservados frente a los riesgos de abuso y de acceso ilícito a los mismos. Por otro lado, los datos conservados solo pueden utilizarse para la lucha contra delitos graves o para la prevención de un riesgo concreto para la integridad física, la vida o la libertad de una persona o para la existencia del Estado federal o de un *Land*.

36 En cuarto lugar, dicho órgano jurisdiccional considera que la interpretación del artículo 15, apartado 1, de la Directiva 2002/58 en el sentido de una incompatibilidad general con el Derecho de la Unión de

toda conservación de datos sin motivo puede contravenir la obligación de actuar de los Estados miembros, derivada del derecho a la seguridad consagrado en el artículo 6 de la Carta.

37 En quinto lugar, el órgano jurisdiccional remitente considera que una interpretación del artículo 15 de la Directiva 2002/58 en el sentido de que se opone a una conservación generalizada de datos restringiría considerablemente el margen de maniobra del legislador nacional en un ámbito relacionado con la represión de los delitos y la seguridad pública, que, de conformidad con el artículo 4 TUE, apartado 2, sigue siendo responsabilidad exclusiva de cada Estado miembro.

38 En sexto lugar, el órgano jurisdiccional remitente estima que procede tener en cuenta la jurisprudencia del Tribunal Europeo de Derechos Humanos y señala que este ha declarado que el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales (en lo sucesivo, «CEDH») no se opone a disposiciones nacionales que prevean la interceptación masiva de los flujos transfronterizos de datos, habida cuenta de las amenazas a las que se enfrentan actualmente muchos Estados y de las herramientas tecnológicas en las que pueden apoyarse en la actualidad terroristas y delincuentes para cometer actos reprobables.

39 En estas circunstancias, el Bundesverwaltungsgericht (Tribunal Supremo de lo Contencioso-Administrativo) decidió suspender el procedimiento y plantear al Tribunal de Justicia la siguiente cuestión prejudicial:

«¿Debe interpretarse el artículo 15 de la Directiva [2002/58], a la luz de los artículos 7, 8, 11 y 52, apartado 1, de la [Carta], por un lado, y del artículo 6 de [la Carta] y del artículo 4 [TUE], por otro, en el sentido de que se opone a una normativa nacional que obliga a los proveedores de servicios de comunicaciones electrónicas disponibles al público a conservar los datos de tráfico y de localización de los usuarios finales de dichos servicios, cuando:

1) la obligación en cuestión no está sujeta a ninguna condición específica, ya sea geográfica, temporal o espacial;

2) en el caso de prestación de servicios de telefonía disponibles al público (incluida la transmisión de mensajes breves, multimedia o similares y de llamadas perdidas o no respondidas), la obligación en cuestión tiene por objeto los siguientes datos:

a) el número de teléfono u otra identificación de la línea de origen y de destino y, en caso de redirección o desvío de llamada, de las demás líneas intervinientes;

b) la fecha y hora de inicio y fin de la comunicación o, en caso de transmisión de mensajes breves, multimedia o similares, la hora de envío y recepción del mensaje, con indicación de la zona horaria;

c) datos del servicio utilizado, en caso de que en el marco del servicio telefónico puedan utilizarse distintos servicios;

d) en caso de servicios de telefonía móvil, además:

i) la identificación internacional del usuario móvil para la línea de origen y de destino;

ii) la identificación internacional del terminal de origen y de destino;

iii) la fecha y hora de la primera activación del servicio, con indicación de la zona horaria, en caso de servicios de pago anticipado;

iv) denominación de las células utilizadas al inicio de la comunicación por la línea de origen y de destino;

e) en caso de servicios de telefonía por Internet, además, las direcciones de protocolo de Internet de la línea de origen y de destino y las identificaciones de usuario asignadas;

3) en el caso de prestación de servicios de acceso a Internet disponibles al público, la obligación de almacenamiento tiene por objeto los siguientes datos:

a) la dirección de protocolo de Internet asignada al usuario para cada uso de Internet;

b) una identificación exclusiva de la línea utilizada para el uso de Internet, y la identificación de usuario asignada;

c) la fecha y hora de inicio y fin del uso de Internet con la dirección de protocolo de Internet asignada, con indicación de la zona horaria;

d) en caso de uso móvil, la denominación de la célula utilizada al inicio de la conexión;

4) no se permite almacenar los siguientes datos:

a) el contenido de la comunicación;

b) datos de los sitios web visitados;

c) datos de los servicios de correo electrónico;

d) datos relativos a comunicaciones a o desde determinadas líneas de personas, autoridades u organizaciones de ámbitos sociales o religiosos;

5) el plazo de conservación de los datos de localización, es decir, la denominación de la célula utilizada, es de cuatro semanas; para los demás datos, el plazo es de diez semanas;

6) se garantiza una protección efectiva de los datos almacenados frente a cualquier uso indebido y frente a cualquier acceso no autorizado, y

7) solo se permite la utilización de los datos almacenados con fines de investigación de delitos graves y para la prevención de un riesgo concreto para la vida, la integridad física o la libertad de las personas o para la seguridad de la Federación o de un *Land*, con excepción de la dirección de protocolo de Internet asignada al usuario para cada uso de Internet, cuya utilización se autoriza en el marco de transmisiones de extractos de la base de datos con fines de investigación de cualquier tipo de delito y para prevenir riesgos para la seguridad pública y el orden público y no obstaculizar las funciones de los servicios de inteligencia?»

Procedimiento ante el Tribunal de Justicia

40 Mediante decisión del Presidente del Tribunal de Justicia de 3 de diciembre de 2019, se acordó la acumulación de los asuntos C-793/19 y C-794/19 a efectos de las fases escrita y oral del procedimiento y de la sentencia.

41 Mediante decisión del Presidente del Tribunal de Justicia de 14 de julio de 2020, se suspendió el procedimiento en los asuntos acumulados C-793/19 y C-794/19, con arreglo al artículo 55, apartado 1, letra b), del Reglamento de Procedimiento del Tribunal de Justicia, hasta que se dictara sentencia en el asunto La Quadrature du Net y otros (C-511/18, C-512/18 y C-520/18).

42 Una vez que el Tribunal de Justicia dictó, el 6 de octubre de 2020, su sentencia en el asunto La Quadrature du Net y otros (C-511/18, C-512/18 y C-520/18, EU:C:2020:791), el Presidente del Tribunal de Justicia ordenó, el 8 de octubre de 2020, que se reanudara el procedimiento en los asuntos acumulados C-793/19 y C-794/19.

43 El órgano jurisdiccional remitente, al que la Secretaría había comunicado dicha sentencia, indicó que mantenía su petición de decisión prejudicial.

44 A este respecto, el órgano jurisdiccional remitente observó, en primer lugar, que la obligación de conservación establecida por la normativa controvertida en los litigios principales se refiere a un

número menor de datos y a un período de conservación inferior al previsto por las normativas nacionales controvertidas en los asuntos que dieron lugar a 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). Estas particularidades reducen, en su opinión, la posibilidad de que los datos conservados permitan extraer conclusiones muy precisas sobre la vida privada de las personas cuyos datos se han conservado.

45 A continuación, indicó de nuevo que la normativa nacional controvertida en los litigios principales garantiza una protección eficaz de los datos conservados contra los riesgos de abuso y de acceso ilícito.

46 Por último, señaló que subsisten dudas acerca de la compatibilidad con el Derecho de la Unión de la conservación de las direcciones IP prevista por la normativa nacional controvertida en los litigios principales, debido a una incoherencia entre los apartados 155 y 168 de 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). Así, según el órgano jurisdiccional remitente, de dicha sentencia se deriva la duda de si el Tribunal de Justicia exige, para la conservación de las direcciones IP, un motivo de conservación relacionado con el objetivo de salvaguardia de la seguridad nacional, de lucha contra la delincuencia grave o de prevención de amenazas graves contra la seguridad pública, como se desprende del apartado 168 de dicha sentencia, o si la conservación de las direcciones IP está permitida incluso a falta de motivo concreto, ya que solo la utilización de los datos conservados está limitada por dichos objetivos, como se desprende del apartado 155 de dicha sentencia.

Sobre la cuestión prejudicial

47 Mediante su cuestión prejudicial, el órgano jurisdiccional remitente desea saber, en esencia, si el artículo 15, apartado 1, de la Directiva 2002/58, a la luz de los artículos 6 a 8 y 11 y del artículo 52, apartado l, de la Carta y del artículo 4 TUE, apartado 2, debe interpretarse en el sentido de que se opone a una medida legislativa nacional que, salvo determinadas excepciones, impone a los proveedores de servicios de comunicaciones electrónicas disponibles al público, con los fines enumerados en el artículo 15, apartado 1, de dicha Directiva, y en particular para la represión de las infracciones penales graves o la prevención de un riesgo concreto para la seguridad nacional, la conservación generalizada e indiferenciada de los datos esenciales de tráfico y de localización de los usuarios finales de estos servicios, estableciendo un período de conservación de varias semanas y normas destinadas a garantizar una protección eficaz de los datos conservados contra los riesgos de abuso y contra cualquier acceso ilícito a dichos datos.

Aplicabilidad de la Directiva 2002/58

48 Por lo que respecta a la alegación de Irlanda y de los Gobiernos francés, neerlandés, polaco y sueco de que la normativa nacional controvertida en los litigios principales, en la medida en que fue adoptada en particular con el fin de salvaguardar la seguridad nacional, no está comprendida en el ámbito de aplicación de la Directiva 2002/58, basta con recordar que una normativa nacional que obliga a los proveedores de servicios de comunicaciones electrónicas a conservar datos de tráfico y de localización a efectos, en particular, de la protección de la seguridad nacional y de la lucha contra la delincuencia, como la controvertida en los litigios principales, está comprendida en el ámbito de aplicación de la Directiva 2002/58 (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 104.

Interpretación del artículo 15, apartado 1, de la Directiva 2002/58

Recordatorio de los principios derivados de la jurisprudencia del Tribunal de Justicia

49 Según reiterada jurisprudencia, para la interpretación de una disposición del Derecho de la Unión, no solo hay que referirse al tenor de esta, sino también tener en cuenta su contexto y los objetivos perseguidos por la normativa de la que forma parte, así como tomar en consideración, en especial, la génesis de esa normativa (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 32 y jurisprudencia citada).

50 Del propio tenor del artículo 15, apartado 1, de la Directiva 2002/58 se desprende que las medidas legales que esta autoriza a los Estados miembros a adoptar, en las condiciones que en ella se establecen, únicamente pueden ir dirigidas a «limitar el alcance» de los derechos y las obligaciones establecidos en particular en los artículos 5, 6 y 9 de la Directiva 2002/58 (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 33).

51 En cuanto al sistema instaurado por la citada Directiva y en el que se inserta su artículo 15, apartado 1, procede recordar que, en virtud del artículo 5, apartado 1, frases primera y segunda, de dicha Directiva, los Estados miembros están obligados a garantizar, mediante su legislación nacional, la confidencialidad de las comunicaciones realizadas a través de las redes públicas de comunicaciones y de los servicios de comunicaciones electrónicas disponibles al público, así como la confidencialidad de los datos de tráfico asociados a ellas. En particular, están obligados a prohibir 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 artículo 15, apartado 1, de la misma Directiva (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 34).

52 A este respecto, el Tribunal de Justicia ya ha declarado que el artículo 5, apartado 1, de la Directiva 2002/58 consagra el principio de confidencialidad tanto de las comunicaciones electrónicas como de los datos de tráfico asociados a ellas e implica, en particular, la prohibición, en principio, de que cualquier persona distinta de los usuarios almacene esas comunicaciones y datos sin el consentimiento de estos (sentencias 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 107, y de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 35).

53 La citada disposición refleja el objetivo perseguido por el legislador de la Unión al adoptar la Directiva 2002/58. En efecto, de la exposición de motivos de la propuesta de Directiva del Parlamento Europeo y del Consejo relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas [COM(2000) 385 final], que dio lugar a la Directiva 2002/58, se desprende que el legislador de la Unión pretendió que «[siguiera] estando garantizado un nivel elevado de protección de los datos personales y la intimidad para todos los servicios de comunicaciones electrónicas con independencia de la tecnología utilizada». De esta manera, la citada Directiva tiene por finalidad, como se infiere de sus considerandos 6 y 7, proteger a los usuarios de los servicios de comunicaciones electrónicas frente a los riesgos que suponen para sus datos personales y su intimidad las nuevas tecnologías y, en especial, la creciente capacidad de almacenamiento y tratamiento informático de datos. En particular, como se dice en el considerando 2 de la misma Directiva, la voluntad del legislador de la Unión es garantizar el pleno respeto de los derechos reconocidos en los artículos 7 y 8 de la Carta, relativos, respectivamente, al respeto de la vida privada y a la protección de datos de carácter personal (véase, en este sentido, la sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 36 y jurisprudencia citada).

54 A través de la adopción de la Directiva 2002/58, el legislador de la Unión concretó esos derechos, de suerte que los usuarios de los medios de comunicaciones electrónicas tienen derecho a contar con que, en principio, de no mediar su consentimiento, sus comunicaciones y los datos relativos a ellas permanezcan anónimos y no puedan registrarse (sentencias 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 109, y de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 37).

55 Por lo que se refiere al tratamiento y almacenamiento por parte de los proveedores de servicios de comunicaciones electrónicas de los datos de tráfico relativos a abonados y usuarios, el artículo 6 de la Directiva 2002/58 establece, en su apartado 1, que esos datos deberán eliminarse o hacerse anónimos cuando ya no sean necesarios para la transmisión de una comunicación e indica, en su apartado 2, que podrán ser tratados los datos de tráfico necesarios a efectos de la facturación de los abonados y los pagos de las interconexiones solamente hasta la expiración del plazo durante el cual pueda impugnarse legalmente la factura o exigirse el pago. En cuanto a los datos de localización distintos de los datos de

tráfico, el artículo 9, apartado 1, de dicha Directiva establece que esos datos solo podrán tratarse en ciertas condiciones, si se hacen anónimos, o previo consentimiento de los usuarios o abonados.

56 Por lo tanto, la Directiva 2002/58 no se limita a regular el acceso a tales datos mediante garantías dirigidas a prevenir los abusos, sino que también consagra, en particular, el principio de prohibición de su almacenamiento por terceros (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 39).

57 En la medida en que el artículo 15, apartado 1, de la Directiva 2002/58 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 esta Directiva, como los derivados de los principios de confidencialidad de las comunicaciones y de la prohibición de almacenamiento de los datos asociados a ellas, recordados en el apartado 52 de la presente sentencia, tal disposición 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 y, en particular, a la prohibición de almacenar esos datos, prevista en el artículo 5 de la citada Directiva, se convierta en la regla si no se quiere privar en gran medida a esta última disposición de su alcance (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 40 y jurisprudencia citada).

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

59 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 la Carta. A este respecto, el Tribunal de Justicia ya ha declarado que la obligación impuesta por un Estado miembro a los proveedores de servicios de comunicaciones electrónicas, mediante una normativa nacional, de conservar los datos de tráfico con el fin de hacerlos accesibles, en su caso, a las autoridades nacionales competentes suscita dudas en cuanto al cumplimiento no solo de los artículos 7 y 8 de la Carta, sino también del artículo 11 de la Carta, relativo a la libertad de expresión, libertad que constituye uno de los fundamentos esenciales de una sociedad democrática y pluralista y forma parte de los valores en los que se basa la Unión Europea, con arreglo al artículo 2 TUE (véase, en este sentido, la sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartados 42 y 43 y jurisprudencia citada).

60 Debe precisarse a este respecto que la conservación de los datos de tráfico y de localización constituye, por sí sola, por una parte, una excepción a la prohibición, establecida en el artículo 5, apartado 1, de la Directiva 2002/58, de que cualquier persona distinta de los usuarios almacene dichos datos y, por otra parte, una injerencia en los derechos fundamentales al respeto de la vida privada y a la protección de datos de carácter personal, consagrados en los artículos 7 y 8 de la Carta, siendo irrelevante que la información relativa a la vida privada de que se trate tenga o no carácter sensible, que los interesados hayan sufrido o no inconvenientes en razón de tal injerencia, o si los datos conservados serán o no utilizados posteriormente (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 44 y jurisprudencia citada).

61 Esta conclusión parece tanto más justificada cuanto que los datos de tráfico y de localización pueden revelar información sobre un número considerable de aspectos de la vida privada de las personas de que se trate, incluida información de carácter sensible, como la orientación sexual, las opiniones políticas, las creencias religiosas, filosóficas, sociales u otras y el estado de salud, dado que estos datos gozan, además, de una protección particular en el Derecho de la Unión. Considerados en su conjunto,

estos datos pueden permitir extraer conclusiones 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. En particular, estos datos proporcionan medios para determinar el perfil de las personas afectadas, información tan sensible, a la luz del respeto de la vida privada, como el propio contenido de las comunicaciones (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 45 y jurisprudencia citada).

62 En consecuencia, por una parte, la conservación de datos de tráfico y de localización con fines policiales puede vulnerar el derecho al respeto de las comunicaciones, consagrado en el artículo 7 de la Carta, y disuadir a los usuarios de los medios de comunicaciones electrónicas de ejercer su libertad de expresión, garantizada por el artículo 11 de la Carta, efectos que son especialmente graves, dada la cantidad y la variedad de datos conservados. Por otra parte, en vista de la gran cantidad de datos de tráfico y de localización que pueden conservarse de manera continua mediante una medida de conservación generalizada e indiferenciada y del carácter sensible de la información que esos datos pueden proporcionar, su mera conservación por parte de los proveedores de servicios de comunicaciones electrónicas conlleva riesgos de abuso y de acceso ilícito (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 46 y jurisprudencia citada).

63 Ahora bien, en la medida en que permite a los Estados miembros limitar los derechos y las obligaciones mencionados en los apartados 51 a 54 de la presente sentencia, el artículo 15, apartado 1, de la Directiva 2002/58 refleja el hecho de que los derechos consagrados en los artículos 7, 8 y 11 de la Carta no constituyen prerrogativas absolutas, sino que deben considerarse de acuerdo con su función en la sociedad. En efecto, como se desprende del artículo 52, apartado 1, de la Carta, esta admite limitaciones al ejercicio de esos derechos, siempre que se establezcan por ley, respeten el contenido esencial de los citados derechos y, ajustándose al principio de proporcionalidad, sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás. De este modo, la interpretación del artículo 15, apartado 1, de la Directiva 2002/58 a la luz de la Carta exige tener en cuenta asimismo la importancia de los derechos consagrados en los artículos 3, 4, 6 y 7 de la Carta y la que presentan los objetivos de protección de la seguridad nacional y de lucha contra la delincuencia grave al contribuir a la protección de los derechos y de las libertades de terceros (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 48 y jurisprudencia citada).

64 De esta manera, por lo que respecta, específicamente, a la lucha efectiva contra los delitos perpetrados, en particular, contra los menores y otras personas vulnerables, debe tenerse en cuenta que del artículo 7 de la Carta pueden resultar obligaciones positivas que incumban a los poderes públicos, con miras a la adopción de medidas jurídicas dirigidas a proteger la vida privada y familiar. Estas obligaciones pueden resultar asimismo de dicho artículo 7 por lo que se refiere a la protección del domicilio y de las comunicaciones, así como de los artículos 3 y 4 en lo tocante a la protección de la integridad física y psíquica de la persona y a la prohibición de la tortura y de los tratos inhumanos o degradantes (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 49 y jurisprudencia citada).

65 En consecuencia, frente a estas diferentes obligaciones positivas, conviene proceder a una conciliación de los distintos intereses legítimos y derechos en juego, y establecer un marco jurídico que permita esta conciliación (véase, en este sentido, la sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 50 y jurisprudencia citada).

66 En este marco, de los propios términos del artículo 15, apartado 1, primera frase, de la Directiva 2002/58 se infiere que los Estados miembros podrán adoptar una medida que suponga una excepción al principio de confidencialidad al que se ha hecho referencia en el apartado 52 de la presente sentencia, cuando tal medida sea «necesaria, proporcionada y apropiada en una sociedad democrática», mientras que el considerando 11 de esta Directiva precisa a tal efecto que una medida de esta naturaleza debe ser «rigurosamente» proporcionada al objetivo que pretende lograr.

67 A este respecto, debe recordarse que la protección del derecho fundamental a la intimidad exige, conforme a la jurisprudencia reiterada del Tribunal de Justicia, que las excepciones a la protección de los datos personales y las restricciones a dicha protección se establezcan sin sobrepasar los límites de lo estrictamente necesario. Además, no puede perseguirse un objetivo de interés general sin tener en cuenta que debe conciliarse con los derechos fundamentales afectados por la medida, efectuando una ponderación equilibrada entre, por una parte, el objetivo de interés general y, por otra parte, los intereses y derechos de que se trate (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 52 y jurisprudencia citada).

68 Más concretamente, de la jurisprudencia del Tribunal de Justicia se desprende 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 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 53 y jurisprudencia citada).

69 Para cumplir el requisito de proporcionalidad, una normativa nacional 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 y, en particular, 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. La necesidad de disponer de esas garantías es aún más importante cuando los datos personales se someten a un tratamiento automatizado, sobre todo cuando existe un riesgo elevado de acceso ilícito a ellos. Estas consideraciones son especialmente aplicables cuando está en juego la protección de esa categoría particular de datos personales que son los datos sensibles (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 54 y jurisprudencia citada).

70 De este modo, una normativa nacional que establezca la conservación de los datos de carácter personal debe responder en todo caso a criterios objetivos y ha de existir una relación entre los datos que deban conservarse y el objetivo que se pretende lograr (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 55 y jurisprudencia citada).

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

72 Así pues, por lo que respecta a la salvaguardia de la seguridad nacional, cuya importancia rebasa la de los demás objetivos contemplados en el artículo 15, apartado 1, de la Directiva 2002/58, el Tribunal de Justicia ha declarado que esta disposición, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta, no se opone a medidas legislativas que permitan, a efectos de la protección de la seguridad nacional, recurrir a un requerimiento efectuado a los proveedores de servicios de comunicaciones electrónicas para que procedan a una conservación generalizada e indiferenciada de los datos de tráfico y de localización, en situaciones en las que el Estado miembro en cuestión se enfrenta a una amenaza grave para la seguridad nacional que resulte real y actual o previsible, pudiendo ser objeto la decisión que contenga dicho requerimiento de un control efectivo bien por un órgano jurisdiccional, bien por una entidad administrativa independiente, cuya decisión tenga carácter vinculante, que tenga por objeto comprobar la existencia de una de estas situaciones, así como el respecto de las condiciones y de las garantías que deben establecerse, y teniendo en cuenta que dicho requerimiento únicamente podrá expedirse por un período temporalmente limitado a lo estrictamente necesario, pero que podrá

renovarse en caso de que persista dicha amenaza (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 58 y jurisprudencia citada).

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

74 Por lo que respecta al objetivo de lucha contra la delincuencia grave, el Tribunal de Justicia ha declarado que una normativa nacional que establece, a tales efectos, la conservación generalizada e indiferenciada de los datos de tráfico y de localización excede de los límites de lo estrictamente necesario y no puede considerarse justificada en una sociedad democrática. En efecto, habida cuenta del carácter sensible de la información que pueden proporcionar los datos de tráfico y de localización, la confidencialidad de estos es fundamental para el derecho al respeto de la vida privada. De este modo, y teniendo en cuenta, por una parte, los efectos disuasorios sobre el ejercicio de los derechos fundamentales consagrados en los artículos 7 y 11 de la Carta, a los que se ha hecho referencia en el apartado 62 de la presente sentencia, que la conservación de estos datos puede acarrear y, por otra parte, la gravedad de la injerencia que supone dicha conservación, es importante que en una sociedad democrática tal conservación constituya, como prevé el sistema establecido por la Directiva 2002/58, la excepción y no la regla y que esos datos no puedan ser objeto de una conservación sistemática y continua. Esta conclusión se impone incluso respecto de los objetivos de lucha contra la delincuencia grave y de prevención de las amenazas graves contra la seguridad pública, así como de la importancia que se les debe reconocer (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 65 y jurisprudencia citada).

75 En cambio, el Tribunal de Justicia ha precisado 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, no se opone a medidas legislativas que establezcan, a efectos de la lucha contra la delincuencia grave y de la prevención de amenazas graves contra la seguridad pública,

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

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

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

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

siempre que dichas medidas garanticen, mediante normas claras y precisas, que la conservación de los datos en cuestión está supeditada al respeto de las condiciones materiales y procesales correspondientes y que las personas afectadas disponen de garantías efectivas contra los riesgos de abuso (sentencias 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, y de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 67).

Medida que establece, durante un período de varias semanas, una conservación generalizada e indiferenciada de la mayor parte de los datos de tráfico y de localización

76 Las características de la normativa nacional controvertida en los litigios principales, puestas de relieve por el órgano jurisdiccional remitente, deben examinarse a la luz de estas consideraciones de principio.

77 En primer lugar, por lo que respecta al alcance de los datos conservados, de la resolución de remisión se desprende que, en el marco de la prestación de servicios telefónicos, la obligación de conservación establecida por dicha normativa se refiere, en particular, a los datos necesarios para identificar el origen de una comunicación y el destino de esta, la fecha y hora del inicio y del fin de la comunicación o —en caso de comunicación por SMS, mensaje multimedia o mensaje similar— el momento del envío y de la recepción del mensaje, así como, en el caso de la utilización del móvil, la designación de las células utilizadas al inicio de la comunicación por la línea de origen y de destino. En el marco de la prestación de servicios de acceso a Internet, la obligación de conservación se refiere, entre otras cosas, a la dirección IP atribuida al abonado, la fecha y hora de inicio y fin del uso de Internet desde la dirección IP atribuida y, en caso de utilización del móvil, la designación de las células utilizadas al inicio de la conexión a Internet. También se conservarán los datos que permiten conocer la posición geográfica y las direcciones de radiación máxima de las antenas que sirven a la célula telefónica de que se trate.

78 Si bien la normativa nacional controvertida en los litigios principales excluye de la obligación de conservación el contenido de la comunicación y los datos relativos a los sitios de Internet consultados y solo exige la conservación del identificador de célula al inicio de la comunicación, procede señalar que lo mismo sucedía, en esencia, con las normativas nacionales de transposición de la Directiva 2006/24 controvertidas en los asuntos que dieron lugar a 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). Pues bien, a pesar de estas limitaciones, el Tribunal de Justicia declaró en esa sentencia que las categorías de datos conservados en virtud de dicha Directiva y de esas normativas nacionales podían permitir extraer conclusiones muy precisas sobre la vida privada de las personas afectadas, como los hábitos de la vida cotidiana, los lugares de residencia permanentes o temporales, los desplazamientos diarios u otros, las actividades ejercidas, sus relaciones sociales y los círculos sociales que frecuentan, y, en particular, facilitar los medios para determinar el perfil de esas personas.

79 Además, es preciso señalar que, aunque la normativa controvertida en los litigios principales no comprende los datos relativos a los sitios de Internet consultados, prevé no obstante la conservación de las direcciones IP. Pues bien, puesto que estas direcciones pueden utilizarse para llevar a cabo, en particular, el rastreo exhaustivo de la secuencia de navegación de un internauta y, en consecuencia, de su actividad en línea, tales datos permiten establecer el perfil detallado de este. Por lo tanto, la conservación y el análisis de dichas direcciones IP que precisa ese rastreo constituyen injerencias graves en los derechos fundamentales del internauta consagrados en los artículos 7 y 8 de la Carta (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 153).

80 Además, como ha señalado SpaceNet en sus observaciones escritas, los datos relativos a los servicios de correo electrónico, aunque no estén cubiertos por la obligación de conservación establecida por la normativa controvertida en los litigios principales, solo representan una ínfima parte de los datos de que se trata.

81 Así, como ha señalado el Abogado General, en esencia, en el punto 60 de sus conclusiones, la obligación de conservación establecida por la normativa nacional controvertida en los litigios principales se extiende a un amplísimo conjunto de datos de tráfico y de localización, que corresponde, fundamentalmente, a los que dieron lugar a la reiterada jurisprudencia recordada en el apartado 78 de la presente sentencia.

82 Además, en respuesta a una pregunta formulada en la vista, el Gobierno alemán precisó que solo 1 300 entidades estaban inscritas en la lista de personas, autoridades y organizaciones de carácter social o religioso cuyos datos relativos a las comunicaciones electrónicas no se conservan en virtud de los artículos 99, apartado 2, y 113b, apartado 6, de la TKG, lo que representa manifiestamente una parte reducida del conjunto de usuarios de los servicios de telecomunicaciones en Alemania cuyos datos

están sujetos a la obligación de conservación prevista por la normativa nacional controvertida en los litigios principales. Así, se conservan, en particular, los datos de los usuarios sujetos al secreto profesional, como los abogados, los médicos y los periodistas.

83 Por lo tanto, de la resolución de remisión se desprende que la conservación de los datos de tráfico y de localización prevista por dicha normativa nacional afecta a casi todas las personas que componen la población sin que estas se encuentren, ni siquiera indirectamente, en una situación que pueda dar lugar a acciones penales. Asimismo, exige la conservación, sin motivo, generalizada y no diferenciada desde el punto de vista personal, temporal y geográfico, de la parte esencial de los datos de tráfico y de localización cuyo alcance corresponde, en esencia, al de los datos conservados en los asuntos que dieron lugar a la jurisprudencia mencionada en el apartado 78 de la presente sentencia.

84 Por lo tanto, habida cuenta de la jurisprudencia citada en el apartado 75 de la presente sentencia, una obligación de conservación de datos como la controvertida en los litigios principales no puede considerarse una conservación selectiva de los datos, contrariamente a lo que sostiene el Gobierno alemán.

85 En segundo lugar, por lo que respecta al período de conservación de los datos, del artículo 15, apartado 1, segunda frase, de la Directiva 2002/58 se desprende que el período de conservación previsto por una medida nacional que impone una obligación de conservación generalizada e indiferenciada es, ciertamente, un factor pertinente, entre otros, para determinar si el Derecho de la Unión se opone a tal medida, dado que dicha frase exige que esa duración sea «limitada».

86 Pues bien, en el caso de autos, es cierto que estos períodos, que ascienden, según el artículo 113b, apartado 1, de la TKG, a cuatro semanas para los datos de localización y diez semanas para los demás datos, son sensiblemente más cortos que los previstos por las normativas nacionales que imponen una obligación de conservación generalizada e indiferenciada examinadas por el Tribunal de Justicia en sus sentencias de 21 de diciembre de 2016, Tele2 Sverige y Watson y otros (C-203/15 y C-698/15, EU:C:2016:970); 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), y de 5 de abril de 2022, Commissioner of An Garda Síochána y otros (C-140/20, EU:C:2022:258).

87 No obstante, como se desprende de la jurisprudencia citada en el apartado 61 de la presente sentencia, la gravedad de la injerencia se deriva del riesgo, en particular habida cuenta del número y la variedad de los datos conservados, considerados en su conjunto, de que estos permitan extraer conclusiones muy precisas sobre la vida privada de la persona o personas cuyos datos se han conservado y, en concreto, proporcionen los medios para establecer el perfil de la persona o personas afectadas, que, en lo que respecta al derecho al respeto de la vida privada, es una información tan sensible como el propio contenido de las comunicaciones.

88 Por tanto, la conservación de los datos de tráfico o de localización, que pueden proporcionar 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 de conservación, de la cantidad y de la naturaleza de los datos conservados, cuando ese conjunto de datos pueda permitir extraer conclusiones muy precisas sobre la vida privada de la persona o personas afectadas [véase, en relación con el acceso a tales datos, 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 39].

89 A este respecto, incluso la conservación de una cantidad limitada de datos de tráfico o de localización o la conservación de esos datos durante un período breve pueden facilitar información muy precisa sobre la vida privada de un usuario de un medio de comunicación electrónica. Además, la cantidad de los datos disponibles y la información muy precisa sobre la vida privada de la persona afectada que de ellos resulta solo pueden apreciarse después de consultar dichos datos. Pues bien, la injerencia resultante de la conservación de dichos datos se produce necesariamente antes de que puedan consultarse los datos y la información que se deriva de ellos. Así, la apreciación de la gravedad de la injerencia que constituye la conservación se efectúa necesariamente en función del riesgo para la vida privada de las personas afectadas que suele corresponder a la categoría de datos conservados, 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 [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 40].

90 En el caso de autos, como se desprende del apartado 77 de la presente sentencia y como se confirmó en la vista, un conjunto de datos de tráfico y de localización conservados durante, respectivamente, diez semanas y cuatro semanas puede permitir extraer conclusiones muy precisas sobre la vida privada de las personas cuyos datos se conservan, como los hábitos de la vida cotidiana, los lugares de estancia permanentes o temporales, los desplazamientos diarios u otros, las actividades ejercidas, las relaciones sociales de esas personas y los medios sociales que frecuentan, y, en particular, establecer un perfil de estas personas.

91 En tercer lugar, por lo que respecta a las garantías establecidas por la normativa nacional controvertida en los litigios principales, dirigidas a proteger los datos conservados contra los riesgos de abuso y contra todo acceso ilícito, procede señalar que la conservación de esos datos y el acceso a ellos constituyen, como se desprende de la jurisprudencia recordada en el apartado 60 de la presente sentencia, injerencias distintas en los derechos fundamentales garantizados por los artículos 7 y 11 de la Carta que requieren una justificación distinta, con arreglo al artículo 52, apartado 1, de esta. Por lo tanto, una normativa nacional que cumpla estrictamente los requisitos formulados por la jurisprudencia relativa a la Directiva 2002/58 en materia de acceso a los datos conservados no puede, por naturaleza, ni limitar ni menos aún subsanar la injerencia grave originada por la conservación generalizada de tales datos con arreglo a esa normativa nacional en los derechos garantizados por los artículos 5 y 6 de dicha Directiva y por los derechos fundamentales que quedaron determinados mediante estos artículos (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 47).

92 En cuarto y último lugar, por lo que respecta a la alegación de la Comisión Europea de que la delincuencia particularmente grave podría asimilarse a una amenaza para la seguridad nacional, el Tribunal de Justicia ya ha declarado que el objetivo de protección de la seguridad nacional corresponde al interés primordial de proteger las funciones esenciales del Estado y los intereses fundamentales de la sociedad e incluye la prevención y la represión de actividades que puedan desestabilizar gravemente las estructuras constitucionales, políticas, económicas o sociales fundamentales de un país, y, en particular, amenazar directamente a la sociedad, a la población o al propio Estado, tales como las actividades terroristas (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 61 y jurisprudencia citada).

93 A diferencia de la delincuencia, aunque sea especialmente grave, una amenaza para la seguridad nacional debe ser real y actual, o cuando menos previsible, lo que supone que surjan circunstancias suficientemente concretas para poder justificar una medida de conservación generalizada e indiferenciada de datos de tráfico y de localización, durante un plazo limitado. Así pues, tal amenaza se distingue, por su naturaleza, su gravedad y el carácter específico de las circunstancias que la forman, del riesgo general y permanente de que surjan tensiones o perturbaciones, incluso graves, que afecten a la seguridad pública o del riesgo de delitos graves (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 62 y jurisprudencia citada).

94 La delincuencia, aunque sea especialmente grave, no puede asimilarse, pues, a una amenaza para la seguridad nacional. En efecto, tal asimilación podría implicar la introducción de una categoría intermedia entre la seguridad nacional y la seguridad pública para aplicar a la segunda las exigencias inherentes a la primera (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 63).

Medidas que prevén una conservación selectiva, una conservación rápida o una conservación de direcciones IP

95 Varios Gobiernos, entre ellos el Gobierno francés, subrayan que solo una conservación generalizada e indiferenciada permite la consecución eficaz de los objetivos perseguidos por las medidas de conservación, mientras que el Gobierno alemán sostiene, en esencia, que tal conclusión no queda

desvirtuada por el hecho de que los Estados miembros puedan recurrir a las medidas de conservación selectiva y de conservación rápida contempladas en el apartado 75 de la presente sentencia.

96 A este respecto, se ha de señalar, en primer lugar, que la eficacia de las acciones penales depende generalmente no de un solo medio de investigación, sino de todos los medios de investigación que se hallen a disposición de las autoridades nacionales competentes a los referidos efectos (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 69).

97 En segundo lugar, 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, tal como ha sido interpretado por la jurisprudencia recordada en el apartado 75 de la presente sentencia, permite a los Estados miembros adoptar, a efectos de la lucha contra la delincuencia grave y de la prevención de amenazas graves contra la seguridad pública, no solo medidas que establezcan una conservación selectiva y una conservación rápida, sino también medidas dirigidas a una conservación generalizada e indiferenciada, por un lado, de los datos relativos a la identidad civil de los usuarios de medios de comunicación electrónica y, por otro, de las direcciones IP atribuidas al origen de una conexión (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 70).

98 A este respecto, consta que la conservación de los datos relativos a la identidad civil de los usuarios de los medios de comunicación electrónica puede contribuir a la lucha contra la delincuencia grave, siempre que esos datos permitan identificar a las personas que han utilizado tales medios en el contexto de la preparación o la comisión de un acto delictivo grave (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 71).

99 Pues bien, la Directiva 2002/58 no se opone, a efectos de la lucha contra la criminalidad en general, a la conservación generalizada de los datos relativos a la identidad civil. En tal contexto, debe observarse que ni esta Directiva ni ningún otro acto del Derecho de la Unión se oponen a una normativa nacional, que tenga por objeto la lucha contra la delincuencia grave, en virtud de la cual la adquisición de un medio de comunicación electrónica, como una tarjeta SIM de prepago, está supeditada a la comprobación de documentos oficiales que acrediten la identidad del comprador y al registro, por el vendedor, de la información obtenida por tal vía, estando el vendedor, en su caso, obligado a permitir a las autoridades nacionales competentes que accedan a esa información (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 72).

100 Además, procede recordar que la conservación generalizada de las direcciones IP del origen de la conexión constituye una injerencia grave en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta, toda vez que tales direcciones IP pueden permitir extraer conclusiones precisas sobre la vida privada del usuario del medio de comunicación electrónica de que se trate y puede tener efectos disuasorios sobre el ejercicio de la libertad de expresión garantizada en el artículo 11 de la Carta. No obstante, respecto de tal conservación, el Tribunal de Justicia ha señalado que debe tenerse en cuenta, a efectos de la necesaria conciliación de los derechos y de los intereses legítimos en cuestión exigida por la jurisprudencia a la que se ha hecho referencia en los apartados 65 a 68 de la presente sentencia, el hecho de que, en caso de un delito cometido en línea y, en particular, en caso de la adquisición, la difusión, la transmisión o la puesta a disposición en línea de pornografía infantil, en el sentido del artículo 2, letra c), de la Directiva 2011/93/UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil y por la que se sustituye la Decisión Marco 2004/68/JAI del Consejo (DO 2011, L 335, p. 1; corrección de errores en DO 2012, L 18, p. 7), la dirección IP puede constituir el único método de investigación para identificar a la persona a la que se atribuyó esa dirección en el momento en que se cometió dicho delito (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 73).

101 En estas circunstancias, si bien es cierto que una medida legislativa que establece la conservación de las direcciones IP del conjunto de las personas físicas propietarias de un equipo terminal desde el que puede accederse a Internet se dirigiría a personas que a primera vista no presentan ninguna relación, en el sentido de la jurisprudencia citada en el apartado 70 de la presente sentencia, con los objetivos perseguidos y que, conforme a lo expuesto en el apartado 54 de la presente sentencia, los internautas

tienen derecho a esperar, con arreglo a los artículos 7 y 8 de la Carta, que su identidad no sea, en principio, revelada, una medida legislativa que establece únicamente la conservación generalizada e indiferenciada de las direcciones IP atribuidas al origen de una conexión no parece, en principio, contraria al artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8 y 11 y el artículo 52, apartado 1, de la Carta, siempre que esta posibilidad esté sujeta al riguroso respeto de las condiciones materiales y procesales que deben regular la utilización de tales datos (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:2020:79, apartado 155).

102 Habida cuenta del carácter grave de la injerencia en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta que supone esta conservación, solo la lucha contra la delincuencia grave y la prevención de las amenazas graves a la seguridad pública pueden, al igual que la protección de la seguridad nacional, justificar esta injerencia. Además, la duración de conservación no puede exceder de lo estrictamente necesario habida cuenta del objetivo perseguido. Por último, una medida de esta naturaleza debe prever condiciones y garantías estrictas por lo que se refiere a la explotación de dichos datos, en particular mediante un rastreo, en lo que respecta a las comunicaciones y actividades efectuadas en línea por las personas afectadas (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 156).

103 Así, contrariamente a lo que ha señalado el órgano jurisdiccional remitente, no existe ninguna tensión entre los apartados 155 y 168 de 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). En efecto, como ha señalado en esencia el Abogado General en los puntos 81 y 82 de sus conclusiones, de este apartado 155, en relación con el apartado 156 y el apartado 168 de dicha sentencia, se desprende claramente que solo la lucha contra la delincuencia grave y la prevención de amenazas graves a la seguridad pública pueden, al igual que la protección de la seguridad nacional, justificar la conservación generalizada e indiferenciada de las direcciones IP atribuidas al origen de una conexión, con independencia de si las personas afectadas pueden tener una relación, al menos indirecta, con los objetivos que se persiguen.

104 En tercer lugar, por lo que respecta a las medidas legislativas que prevén una conservación selectiva y una conservación rápida de los datos de tráfico y de localización, algunas consideraciones expuestas por los Estados miembros contra tales medidas ponen de manifiesto una comprensión más restrictiva del alcance de estas medidas que la adoptada por la jurisprudencia mencionada en el apartado 75 de la presente sentencia. En efecto, si bien, conforme a lo que se ha recordado en el apartado 57 de la presente sentencia, esas medidas de conservación deben constituir una excepción dentro del sistema instaurado por la Directiva 2002/58, esta última, interpretada a la luz de los derechos fundamentales consagrados en los artículos 7, 8, 11 y 52, apartado 1, de la Carta, no supedita la posibilidad de expedir un requerimiento que imponga una conservación selectiva al requisito de que se conozcan de antemano los lugares que pueden ser escenario de un acto delictivo grave ni las personas sospechosas de estar implicadas en tal acto. De igual forma, dicha Directiva no exige que el requerimiento que impone una conservación rápida se limite a los sospechosos que ya habían sido antes identificados (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 75).

105 Para empezar, por lo que se refiere a la conservación selectiva, el Tribunal de Justicia ha declarado que el artículo 15, apartado 1, de la Directiva 2002/58 no se opone a una normativa nacional basada en elementos objetivos que permitan dirigirse, por un lado, a las personas cuyos datos de tráfico y de localización puedan presentar una relación, por lo menos indirecta, con delitos graves, contribuir a la lucha contra la delincuencia grave o prevenir un riesgo grave para la seguridad pública o incluso un riesgo para la seguridad nacional (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 76).

106 El Tribunal de Justicia ha señalado al respecto que, si bien tales elementos objetivos pueden variar en función de las medidas adoptadas a efectos de la prevención, la investigación, el descubrimiento y la persecución de la delincuencia grave, dichas personas pueden, en particular, ser aquellas que han sido identificadas previamente, en el marco de procedimientos nacionales aplicables y sobre la base de elementos objetivos y no discriminatorios, como una amenaza para la seguridad pública o la seguridad

nacional del Estado miembro en cuestión (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 77).

107 De esta manera, los Estados miembros tienen la facultad de adoptar medidas de conservación sobre personas a las que se identifica porque están siendo investigadas o están siendo objeto de otras medidas de vigilancia o constan en el registro nacional de antecedentes penales por una condena anterior por delitos graves que pueden implicar un elevado riesgo de reincidencia. Pues bien, si tal identificación se basa en elementos objetivos y no discriminatorios, definidos por el Derecho nacional, la conservación selectiva concerniente a personas identificadas de este modo está justificada (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 78).

108 Por otro lado, una medida de conservación selectiva de datos de tráfico y de localización puede fundarse asimismo, según la elección del legislador nacional y respetándose estrictamente el principio de proporcionalidad, en un criterio geográfico si las autoridades nacionales competentes consideran, sobre la base de elementos objetivos y no discriminatorios, que existe una situación caracterizada por un riesgo elevado de preparación o de comisión de delitos graves en una o varias zonas geográficas. Estas zonas pueden ser, en particular, lugares en los que se produce un número elevado de delitos graves, lugares especialmente expuestos a la comisión de delitos graves, como los lugares o infraestructuras a los que acuden con regularidad un número muy elevado de personas, o incluso lugares estratégicos, como aeropuertos, estaciones de ferrocarril, puertos marítimos o zonas de peajes (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 79 y jurisprudencia citada).

109 Conviene destacar que, según esta jurisprudencia, las autoridades nacionales competentes pueden adoptar, para las zonas mencionadas en el apartado anterior, una medida de conservación selectiva fundada en un criterio geográfico, como, en particular, la tasa media de delincuencia en una zona geográfica, sin que dispongan necesariamente de indicios concretos sobre la preparación o la comisión de delitos graves en las zonas de que se trata. En la medida en que una conservación selectiva fundada en tal criterio puede afectar, en función de los delitos graves contemplados y de la situación específica de los Estados miembros respectivos, tanto a lugares en los que se produce un elevado número de delitos graves como a los lugares especialmente expuestos a la comisión de tales delitos, en principio, tampoco puede dar lugar a discriminaciones, pues el criterio relativo a la tasa media de delincuencia grave no presenta, en sí mismo, ningún vínculo con elementos potencialmente discriminatorios (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 80).

110 Al fin y al cabo, una medida de conservación selectiva referida a lugares o infraestructuras frecuentadas regularmente por un número muy elevado de personas o lugares estratégicos, como aeropuertos, estaciones de ferrocarril, puertos marítimos o zonas de peajes, permite a las autoridades competentes obtener datos de tráfico y, en particular, datos de localización de todas las personas que utilizan en un momento dado un medio de comunicación electrónica en uno de esos lugares. De esta manera, tal medida de conservación selectiva puede permitir a dichas autoridades obtener, mediante el acceso a los datos así conservados, información sobre la presencia de esas personas en los lugares o zonas geográficas objeto de la expresada medida, así como sobre sus desplazamientos entre o dentro de tales lugares o zonas y extraer conclusiones, a efectos de la lucha contra la delincuencia grave, sobre su presencia y su actividad en esos lugares o zonas geográficas en un momento dado durante el período de conservación (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 81).

111 Debe señalarse asimismo que las zonas geográficas a las que se refiere tal conservación selectiva pueden y, en su caso, deben modificarse en función de la evolución de las condiciones que justificaron su selección, permitiendo así, en particular, reaccionar al compás de los progresos en la lucha contra la delincuencia grave. En efecto, el Tribunal de Justicia ya ha declarado que la duración de las medidas de conservación selectiva descritas en los apartados 105 a 110 de la presente sentencia no debe exceder de lo estrictamente necesario habida cuenta del objetivo perseguido, así como de las circunstancias que las justifican, sin perjuicio de que puedan ser renovadas si persiste la necesidad de proceder a dicha conservación (sentencias 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 151, y de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 82).

112 En cuanto a la posibilidad de establecer algún criterio distintivo que no sea ni personal ni geográfico para efectuar una conservación selectiva de datos de tráfico y de localización, no puede excluirse que se tengan en cuenta otros criterios, objetivos y no discriminatorios, para garantizar que el alcance de una conservación selectiva se limite a lo estrictamente necesario y establecer un vínculo, al menos indirecto, entre los delitos graves y las personas cuyos datos van a conservarse. Ahora bien, dado que el artículo 15, apartado 1, de la Directiva 2002/58 se refiere a las medidas legales de los Estados miembros, incumbe a estos últimos y no al Tribunal de Justicia identificar tales criterios, partiendo de la base de que no puede tratarse de reinstaurar de esta manera una conservación generalizada e indiferenciada de los datos de tráfico y de localización (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 83).

113 En cualquier caso, como ha señalado el Abogado General en el punto 50 de sus conclusiones, la eventual existencia de dificultades para definir con precisión los casos y las condiciones en que pueda realizarse una conservación selectiva no justifica que los Estados miembros, haciendo de la excepción una norma, establezcan una conservación generalizada e indiferenciada de datos de tráfico y de localización (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 84).

114 Por lo que respecta, a continuación, a la conservación rápida de los datos de tráfico y de localización tratados y almacenados por los proveedores de servicios de comunicaciones electrónicas de acuerdo con los artículos 5, 6 y 9 de la Directiva 2002/58 o con las medidas legales adoptadas en virtud del artículo 15, apartado 1, de dicha Directiva, procede recordar que tales datos, en principio, deben ser suprimidos o anonimizados, según los casos, al expirar los plazos legales en los que han de tener lugar, de conformidad con las disposiciones nacionales de transposición de la citada Directiva, su tratamiento y almacenamiento. No obstante, el Tribunal de Justicia ha declarado que, durante ese tratamiento y ese almacenamiento, pueden presentarse situaciones en las que surja la necesidad de conservar tales datos más allá de estos plazos para investigar delitos graves o atentados contra la seguridad nacional, tanto en la situación en que esos delitos o atentados ya hayan podido comprobarse como en aquella en la que su existencia pueda sospecharse fundadamente al término de un examen objetivo del conjunto de las circunstancias pertinentes (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 85).

115 En tal situación, habida cuenta de la conciliación necesaria de los derechos e intereses legítimos en juego a que se refieren los apartados 65 a 68 de la presente sentencia, los Estados miembros pueden establecer, en una normativa adoptada en virtud del artículo 15, apartado 1, de la Directiva 2002/58, la posibilidad de requerir, mediante una decisión de la autoridad competente sujeta a un control jurisdiccional efectivo, a los proveedores de servicios de comunicaciones electrónicas para que procedan, durante un período determinado, a la conservación rápida de los datos de tráfico y de localización de que dispongan (sentencias 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 163, y de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 86).

116 En la medida en que la finalidad de tal conservación rápida ya no se corresponde con las finalidades para las que los datos se recopilaron y conservaron en un principio y en que todo tratamiento de datos debe, con arreglo al artículo 8, apartado 2, de la Carta, efectuarse para fines concretos, los Estados miembros deben especificar en su normativa la finalidad para la que puede efectuarse la conservación rápida de los datos. Habida cuenta del carácter grave de la injerencia en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta que puede suponer dicha conservación, únicamente pueden justificar esta injerencia la lucha contra la delincuencia grave y, *a fortiori*, la protección de la seguridad nacional, siempre que esa medida y el acceso a los datos así conservados no sobrepasen los límites de lo estrictamente necesario, como los enunciados en los apartados 164 a 167 de 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) (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 87).

117 El Tribunal de Justicia ha indicado que una medida de conservación de esta naturaleza no debe limitarse a los datos de las personas identificadas previamente como representativas de una amenaza para la seguridad pública o la seguridad nacional del Estado miembro de que se trate o de personas de las que se sospecha que han cometido un delito grave o un atentado contra la seguridad nacional. En efecto, según el Tribunal de Justicia, respetando el marco establecido por 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, y habida cuenta de las consideraciones que figuran en el apartado 70 de la presente sentencia, dicha medida puede, según lo que elija el legislador y siempre dentro de los límites de lo estrictamente necesario, ampliarse a los datos de tráfico y de localización de personas distintas de las sospechosas de haber planeado o cometido un delito grave o un atentado contra la seguridad nacional, siempre que estos datos puedan, sobre la base de elementos objetivos y no discriminatorios, contribuir a la investigación de tal delito o de tal atentando contra la seguridad nacional, como los datos de la propia víctima o de su entorno social o profesional (sentencias 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 165, y de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 88).

118 De esta manera, una medida legislativa puede autorizar el recurso a un requerimiento efectuado a los proveedores de servicios de comunicaciones electrónicas para que procedan a la conservación rápida de los datos de tráfico y de localización, en particular, de las personas con las que haya estado en contacto una víctima al utilizar los medios de comunicaciones electrónicas de aquellos antes de que se produjera una amenaza grave para la seguridad pública o de que se cometiera un delito grave (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 89).

119 Según la jurisprudencia del Tribunal de Justicia recordada en el apartado 117 de la presente sentencia y en las mismas condiciones a las que se refiere dicho apartado, tal conservación rápida puede ampliarse igualmente a zonas geográficas determinadas tales como los lugares en que se cometió y se preparó el delito o el atentado contra la seguridad nacional de que se trate. Debe observarse que también pueden ser objeto de tal medida los datos de tráfico y de localización relativos al lugar en el que una persona, víctima potencial de un delito grave, haya desaparecido, siempre que dicha medida y el acceso a los datos conservados de este modo respeten los límites de lo estrictamente necesario a efectos de la lucha contra la delincuencia grave o de la protección de la seguridad nacional enunciados en los apartados 164 a 167 de 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) (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 90).

120 Por otra parte, debe señalarse que el artículo 15, apartado 1, de la Directiva 2002/58 no se opone a que las autoridades nacionales competentes ordenen una medida de conservación rápida ya en la primera fase de la investigación relativa a una amenaza grave para la seguridad pública o a un eventual delito grave, a saber, desde el momento en que esas autoridades puedan incoar tal investigación con arreglo a las disposiciones pertinentes del Derecho nacional (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 91).

121 En cuanto a la variedad de las medidas de conservación de datos de tráfico y de localización a que se refiere el apartado 75 de la presente sentencia, no puede obviarse que esas distintas medidas pueden aplicarse conjuntamente, según la elección del legislador nacional y siempre que se respeten los límites de lo estrictamente necesario. En tales condiciones, 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, tal como lo ha interpretado la jurisprudencia sentada en 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), no se opone a una combinación de esas medidas (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 92).

122 En cuarto y último lugar, se impone advertir que la proporcionalidad de las medidas adoptadas en virtud del artículo 15, apartado 1, de la Directiva 2002/58 requiere, según la reiterada jurisprudencia del Tribunal de Justicia a la que se hace referencia sumariamente en 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), la observancia no solo de los requisitos de aptitud y necesidad, sino también de la exigencia relativa al carácter

proporcionado de esas medidas respecto del objetivo perseguido (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 93).

123 De este modo, procede recordar que, en el apartado 51 de su sentencia de 8 de abril de 2014, Digital Rights Ireland y otros (C-293/12 y C-594/12, EU:C:2014:238), el Tribunal de Justicia declaró que, si bien la lucha contra la delincuencia grave reviste una importancia primordial para garantizar la seguridad pública y su eficacia puede depender en gran medida de la utilización de técnicas modernas de investigación, tal objetivo de interés general, por fundamental que sea, no puede por sí solo justificar que se considere necesaria una medida de conservación generalizada e indiferenciada de los datos de tráfico y de localización como la establecida por la Directiva 2006/24 (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 94).

124 De igual forma, el Tribunal de Justicia indicó, en el apartado 145 de 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), que ni siquiera las obligaciones positivas de los Estados miembros que pueden resultar, según el caso, de los artículos 3, 4 y 7 de la Carta y que se refieren, como se ha señalado en el apartado 64 de la presente sentencia, a la adopción de normas que permitan combatir eficazmente los delitos pueden tener por efecto justificar injerencias tan graves, como las que supone una normativa que establece una conservación de los datos de tráfico y de localización, en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta de prácticamente toda la población sin que los datos de las personas afectadas puedan guardar una relación, al menos indirecta, con el objetivo perseguido (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 95).

125 Por otra parte, las sentencias del Tribunal Europeo de Derechos Humanos de 25 de mayo de 2021, Big Brother Watch y otros c. Reino Unido (CE:ECHR:2021:0525JUD 005817013), y de 25 de mayo de 2021, Centrum för Rättvisa c. Suecia (CE:ECHR:2021:0525JUD 003525208), invocadas por algunos Gobiernos en la vista para sostener que el CEDH no se opone a normativas nacionales que establezcan, en esencia, una conservación generalizada e indiferenciada de los datos de tráfico y de localización, no pueden poner en entredicho la interpretación del artículo 15, apartado 1, de la Directiva 2002/58 que se deriva de las consideraciones anteriores. En efecto, en dichas sentencias se trataba de interceptaciones de masas de datos relativos a comunicaciones internacionales. Así, como señaló la Comisión en la vista, el Tribunal Europeo de Derechos Humanos no se pronunció, en dichas sentencias, sobre la conformidad con el CEDH de una conservación generalizada e indiferenciada de datos de tráfico y de localización en el territorio nacional, ni siquiera de una interceptación de gran amplitud de esos datos con fines de prevención, detección e investigación de delitos graves. En cualquier caso, procede recordar que el artículo 52, apartado 3, de la Carta tiene por objeto garantizar la coherencia necesaria entre los derechos contenidos en ella y los correspondientes derechos garantizados por el CEDH, sin perjuicio de la autonomía del Derecho de la Unión y del Tribunal de Justicia de la Unión Europea, de modo que solo deben tenerse en cuenta los correspondientes derechos del CEDH en vista de la interpretación de la Carta, como umbral de protección mínima (sentencia de 17 de diciembre de 2020, Centraal Israëlitisch Consistorie van België y otros, C-336/19, EU:C:2020:1031, apartado 56).

Acceso a los datos conservados de manera generalizada e indiferenciada

126 En la vista, el Gobierno danés sostuvo que las autoridades nacionales competentes deberían poder acceder, a efectos de la lucha contra la delincuencia grave, a los datos de tráfico y de localización que se hayan conservado de manera generalizada e indiferenciada, de acuerdo con la jurisprudencia dimanada de 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 135 a 139, para hacer frente a una amenaza grave contra la seguridad nacional que resulte real y actual o previsible.

127 Procede señalar de entrada que el hecho de autorizar el acceso, a efectos de la lucha contra la delincuencia grave, a datos de tráfico y de localización que se han conservado de manera generalizada e indiferenciada determina que dicho acceso va a depender de circunstancias ajenas a aquel objetivo, en función de que exista o no una amenaza grave para la seguridad nacional en el Estado miembro de que se trate, como la contemplada en el apartado anterior, mientras que, a la vista del objetivo de lucha contra la delincuencia grave que ha de justificar la conservación de esos datos y el acceso a ellos, no

hay nada que justifique una diferencia de trato entre los Estados miembros (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 97).

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

129 Pues bien, la argumentación del Gobierno danés alude a una situación en la que el objetivo de la solicitud de acceso en cuestión, a saber, la lucha contra la delincuencia grave, es de una importancia menor, en la jerarquía de los objetivos de interés general, que la del que justificó la conservación, a saber, la protección de la seguridad nacional. Autorizar, en tal situación, el acceso a los datos conservados sería contrario a la jerarquía de objetivos de interés general sugerida en el apartado anterior y en los apartados 68, 71, 72 y 73 de la presente sentencia (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 99).

130 Debe recalcarse en particular que, conforme a la jurisprudencia recordada en el apartado 74 de la presente sentencia, los datos de tráfico y de localización no pueden ser objeto de una conservación generalizada e indiferenciada a efectos de la lucha contra la delincuencia grave y, por tanto, estos mismos fines no pueden justificar un acceso a los referidos datos. Pues bien, si estos datos han sido excepcionalmente conservados de manera generalizada e indiferenciada, con fines de protección de la seguridad nacional contra una amenaza que resulta real y actual o previsible, en las condiciones mencionadas en el apartado 71 de la presente sentencia, las autoridades nacionales competentes en materia de investigación de los delitos no pueden acceder a dichos datos en el marco de un proceso penal, so pena de privar de todo efecto útil a la prohibición de efectuar tal conservación a efectos de la lucha contra la delincuencia grave, recordada en el apartado 74 antes citado (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 100).

131 Habida cuenta de todas las consideraciones que anteceden, procede responder a la 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 medidas legislativas nacionales que establezcan, con carácter preventivo, a efectos de la lucha contra la delincuencia grave y la prevención de amenazas graves contra la seguridad pública, una conservación generalizada e indiferenciada de los datos de tráfico y de localización. En cambio, dicho artículo 15, apartado 1, 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 medidas legislativas nacionales:

– que permitan, a efectos de la protección de la seguridad nacional, recurrir a un requerimiento efectuado a los proveedores de servicios de comunicaciones electrónicas para que procedan a una conservación generalizada e indiferenciada de los datos de tráfico y de localización, en situaciones en las que el Estado miembro en cuestión se enfrenta a una amenaza grave para la seguridad nacional que resulte real y actual o previsible, pudiendo ser objeto la decisión que contenga dicho requerimiento de un control efectivo bien por un órgano jurisdiccional, bien por una entidad administrativa independiente, cuya decisión tenga carácter vinculante, que tenga por objeto comprobar la existencia de una de estas situaciones, así como el respecto de las condiciones y de las garantías que deben establecerse, y teniendo en cuenta que dicho requerimiento únicamente podrá expedirse por un período temporalmente limitado a lo estrictamente necesario, pero que podrá renovarse en caso de que persista dicha amenaza;

– que prevean, a efectos de la protección de la seguridad nacional, de la lucha contra la delincuencia grave y de la prevención de las amenazas graves contra la seguridad pública, una conservación selectiva de los datos de tráfico y de localización que esté delimitada, sobre la base de elementos objetivos y no discriminatorios, en función de las categorías de personas afectadas

o mediante un criterio geográfico, para un período temporalmente limitado a lo estrictamente necesario, pero que podrá renovarse;

– que prevean, a efectos de la protección de la seguridad nacional, de la lucha contra la delincuencia grave y de la prevención de las amenazas graves contra la seguridad pública, una conservación generalizada e indiferenciada de las direcciones IP atribuidas al origen de una conexión, para un período temporalmente limitado a lo estrictamente necesario;

– que prevean, a efectos de la protección de la seguridad nacional, de la lucha contra la delincuencia y de la protección de la seguridad pública, una conservación generalizada e indiferenciada de los datos relativos a la identidad civil de los usuarios de medios de comunicaciones electrónicas, y

– que permitan, a efectos de la lucha contra la delincuencia grave y, *a fortiori*, de la protección de la seguridad nacional, recurrir a un requerimiento efectuado a los proveedores de servicios de comunicaciones electrónicas, mediante una decisión de la autoridad competente sujeta a un control jurisdiccional efectivo, para que procedan, durante un período determinado, a la conservación rápida de los datos de tráfico y de localización de que dispongan estos proveedores de servicios,

siempre que dichas medidas garanticen, mediante normas claras y precisas, que la conservación de los datos en cuestión está supeditada al respeto de las condiciones materiales y procesales correspondientes y que las personas afectadas disponen de garantías efectivas contra los riesgos de abuso.

Costas

132 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 el artículo 52, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea,

debe interpretarse en el sentido de que:

se opone a medidas legislativas nacionales que establezcan, con carácter preventivo, a efectos de la lucha contra la delincuencia grave y la prevención de amenazas graves contra la seguridad pública, una conservación generalizada e indiferenciada de los datos de tráfico y de localización;

no se opone a medidas legislativas nacionales:

– **que permitan, a efectos de la protección de la seguridad nacional, recurrir a un requerimiento efectuado a los proveedores de servicios de comunicaciones electrónicas para que procedan a una conservación generalizada e indiferenciada de los datos de tráfico y de localización, en situaciones en las que el Estado miembro en cuestión se enfrenta a una amenaza grave para la seguridad nacional que resulte real y actual o previsible, pudiendo ser objeto la decisión que contenga dicho requerimiento de un control efectivo bien por un órgano jurisdiccional, bien por una entidad administrativa independiente, cuya decisión**

tenga carácter vinculante, que tenga por objeto comprobar la existencia de una de estas situaciones, así como el respecto de las condiciones y de las garantías que deben establecerse, y teniendo en cuenta que dicho requerimiento únicamente podrá expedirse por un período temporalmente limitado a lo estrictamente necesario, pero que podrá renovarse en caso de que persista dicha amenaza;

– **que prevean, a efectos de la protección de la seguridad nacional, de la lucha contra la delincuencia grave y de la prevención de las amenazas graves contra la seguridad pública, una conservación selectiva de los datos de tráfico y de localización que esté delimitada, sobre la base de elementos objetivos y no discriminatorios, en función de las categorías de personas afectadas o mediante un criterio geográfico, para un período temporalmente limitado a lo estrictamente necesario, pero que podrá renovarse;**

– **que prevean, a efectos de la protección de la seguridad nacional, de la lucha contra la delincuencia grave y de la prevención de las amenazas graves contra la seguridad pública, una conservación generalizada e indiferenciada de las direcciones IP atribuidas al origen de una conexión, para un período temporalmente limitado a lo estrictamente necesario;**

– **que prevean, a efectos de la protección de la seguridad nacional, de la lucha contra la delincuencia y de la protección de la seguridad pública, una conservación generalizada e indiferenciada de los datos relativos a la identidad civil de los usuarios de medios de comunicaciones electrónicas, y**

– **que permitan, a efectos de la lucha contra la delincuencia grave y, *a fortiori*, de la protección de la seguridad nacional, recurrir a un requerimiento efectuado a los proveedores de servicios de comunicaciones electrónicas, mediante una decisión de la autoridad competente sujeta a un control jurisdiccional efectivo, para que procedan, durante un período determinado, a la conservación rápida de los datos de tráfico y de localización de que dispongan estos proveedores de servicios,**

siempre que dichas medidas garanticen, mediante normas claras y precisas, que la conservación de los datos en cuestión está supeditada al respeto de las condiciones materiales y procesales correspondientes y que las personas afectadas disponen de garantías efectivas contra los riesgos de abuso.

Firmas

---

* Lengua de procedimiento: alemán.