

SENTENCIA DEL TRIBUNAL DE JUSTICIA (Gran Sala)

de 8 de abril de 2014

«Comunicaciones electrónicas — Directiva 2006/24/CE — Servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones — Conservación de datos generados o tratados en relación con la prestación de tales servicios — Validez — Artículos 7, 8 y 11 de la Carta de los Derechos Fundamentales de la Unión Europea»

En los asuntos acumulados C-293/12 y C-594/12,

que tienen por objeto sendas peticiones de decisión prejudicial planteadas, con arreglo al artículo 267 TFUE, por la High Court (Irlanda) y el Verfassungsgerichtshof (Austria), mediante resoluciones de 27 de enero y 28 de noviembre de 2012, respectivamente, recibidas en el Tribunal de Justicia el 11 de junio y el 19 de diciembre de 2012, en los asuntos

Digital Rights Ireland Ltd (asunto C-293/12)

y

Minister for Communications, Marine and Natural Resources,

Minister for Justice, Equality and Law Reform,

Commissioner of the Garda Síochána,

Irlanda,

The Attorney General,

con intervención de:

Irish Human Rights Commission,

y

Kärntner Landesregierung (asunto C-594/12),

Michael Seitlinger,

Christof Tschohl y otros,

EL TRIBUNAL DE JUSTICIA (Gran Sala),

integrado por el Sr. V. Skouris, Presidente, el Sr. K. Lenaerts, Vicepresidente, el Sr. A. Tizzano, la Sra. R. Silva de Lapuerta, los Sres. T. von Danwitz (Ponente), E. Juhász, A. Borg Barthet, C.G. Fernlund y J.L. da Cruz Vilaça, Presidentes de

Sala, y los Sres. A. Rosas, G. Arestis, J.-C. Bonichot, A. Arabadjiev, la Sra. C. Toader y el Sr. C. Vajda, Jueces;

Abogado General: Sr. P. Cruz Villalón;

Secretario: Sr. K. Malacek, administrador;

habiendo considerado los escritos obrantes en autos y celebrada la vista el 9 de julio de 2013;

consideradas las observaciones presentadas:

- en nombre de Digital Rights Ireland Ltd, por los Sres. F. Callanan, SC, y F. Crehan, BL, designados por el Sr. S. McGarr, Solicitor;
- en nombre del Sr. Seitlinger, por el Sr. G. Otto, Rechtsanwalt;
- en nombre del Sr. Tschohl y otros, por el Sr. E. Scheucher, Rechtsanwalt;
- en nombre de la Irish Human Rights Commission, por el Sr. P. Dillon Malone, BL, designado por la Sra. S. Lucey, Solicitor;
- en nombre de Irlanda, por la Sra. E. Creedon y el Sr. D. McGuinness, en calidad de agentes, asistidos por los Sres. E. Regan, SC, y D. Fennelly, JC;
- en nombre del Gobierno austriaco, por los Sres. G. Hesse y G. Kunnert, en calidad de agentes;
- en nombre del Gobierno español, por la Sra. N. Díaz Abad, en calidad de agente;
- en nombre del Gobierno francés, por los Sres. G. de Bergues y D. Colas y por la Sra. B. Beaupère-Manokha, en calidad de agentes;
- en nombre del Gobierno italiano, por la Sra. G. Palmieri, en calidad de agente, asistida por el Sr. A. De Stefano, avvocato dello Stato;
- en nombre del Gobierno polaco, por los Sres. B. Majczyna y M. Szpunar, en calidad de agentes;
- en nombre del Gobierno portugués, por el Sr. L. Inez Fernandes y la Sra. C. Vieira Guerra, en calidad de agentes;
- en nombre del Gobierno del Reino Unido, por el Sr. L. Christie, en calidad de agente, asistido por la Sra. S. Lee, Barrister;
- en nombre del Parlamento Europeo, por los Sres. U. Rösslein y A. Caiola y por la Sra. K. Zejdová, en calidad de agentes;
- en nombre del Consejo de la Unión Europea, por los Sres. J. Monteiro y E. Sitbon y por la Sra. I. Šulce, en calidad de agentes;

— en nombre de la Comisión Europea, por la Sra. D. Maidani y por los Sres. B. Martenczuk y M. Wilderspin, en calidad de agentes;

oídas las conclusiones del Abogado General, presentadas en audiencia pública el 12 de diciembre de 2013;

dicta la siguiente

Sentencia

- 1 Las peticiones de decisión prejudicial tienen por objeto la validez de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE (DO L 105, p. 54).
- 2 La petición planteada por la High Court (asunto C-293/12) se refiere a un litigio entre Digital Rights Ireland Ltd. (en lo sucesivo, «Digital Rights») y el Minister for Communications, Marine and Natural Resources, el Minister for Justice, Equality and Law Reform, el Commissioner of the Garda Síochána, Irlanda y el Attorney General en relación con la legalidad de medidas legislativas y administrativas nacionales sobre la conservación de datos relativos a comunicaciones electrónicas.
- 3 La petición planteada por el Verfassungsgerichtshof (asunto C-594/12) concierne a recursos de inconstitucionalidad interpuestos, respectivamente, ante ese órgano jurisdiccional por el Kärntner Landesregierung (Gobierno del Land de Carintia) y por los Sres. Seitlinger, Tschohl y otros 11 128 demandantes sobre la compatibilidad de la Ley por la que se transpone la Directiva 2006/24 en el ordenamiento jurídico austriaco con la Ley constitucional federal (Bundes-Verfassungsgesetz).

Marco jurídico

Directiva 95/46/CE

- 4 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 L 281, p. 31), tiene por objeto, conforme a su artículo 1, apartado 1, garantizar la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales.
- 5 Por lo que se refiere a la seguridad del tratamiento de tales datos, el artículo 17, apartado 1, de dicha Directiva establece lo siguiente:

«Los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales.

Dichas medidas deberán garantizar, habida cuenta de los conocimientos técnicos existentes y del coste de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse.»

Directiva 2002/58/CE

6 Conforme a su artículo 1, apartado 1, el objetivo 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 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 L 337, p. 11) (en lo sucesivo, «Directiva 2002/58»), consiste en armonizar las disposiciones de los Estados miembros necesarias 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 Unión Europea. En virtud del apartado 2 de dicho artículo, las disposiciones de esa Directiva especifican y completan la Directiva 95/46 a los efectos mencionados en el citado apartado 1.

7 En cuanto a la seguridad del tratamiento de los datos, el artículo 4 de la Directiva 2002/58 dispone lo siguiente:

«1. El proveedor de un servicio de comunicaciones electrónicas disponible para el público deberá adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad de sus servicios, de ser necesario en colaboración con el proveedor de la red pública de comunicaciones por lo que respecta a la seguridad de la red. Considerando las técnicas más avanzadas y el coste de su aplicación, dichas medidas garantizarán un nivel de seguridad adecuado al riesgo existente.

1 *bis.* Sin perjuicio de lo dispuesto en la Directiva 95/46/CE, las medidas a que se refiere el apartado 1, como mínimo:

- garantizarán que solo el personal autorizado tenga acceso a los datos personales para fines autorizados por la ley,
- protegerán los datos personales almacenados o transmitidos de la destrucción accidental o ilícita, la pérdida o alteración accidentales o el almacenamiento, tratamiento, acceso o revelación no autorizados o ilícitos, y

- garantizarán la aplicación efectiva de una política de seguridad con respecto al tratamiento de datos personales.

Las autoridades nacionales competentes podrán examinar las medidas adoptadas por los proveedores de servicios de comunicaciones electrónicas disponibles al público y podrán formular recomendaciones sobre las mejores prácticas con respecto al nivel de seguridad que debería conseguirse con estas medidas.

2. En caso de que exista un riesgo particular de violación de la seguridad de la red, el proveedor de un servicio de comunicaciones electrónicas disponible para el público deberá informar a los abonados sobre dicho riesgo y, cuando el riesgo quede fuera del ámbito de las medidas que deberá tomar el proveedor del servicio, sobre las posibles soluciones, con una indicación de los posibles costes.»

- 8 En lo que respecta a la confidencialidad de las comunicaciones y de los datos de tráfico, el artículo 5, apartados 1 y 3, de dicha Directiva dispone:

«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/CE. 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.»

- 9 A tenor del artículo 6, apartado 1, de la Directiva 2002/58:

«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.»

- 10 El artículo 15 de la Directiva 2002/58 enuncia en su apartado 1:

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

Directiva 2006/24

- 11 Después de haber formulado una consulta a los representantes de las autoridades represivas, a la industria de las comunicaciones electrónicas y a expertos en protección de datos, la Comisión presentó, el 21 de septiembre de 2005, una evaluación del impacto de las opciones políticas relativas a las normas sobre la conservación de datos de tráfico (en lo sucesivo, «evaluación de impacto»). Esta evaluación sirvió de base para la elaboración de la Propuesta de Directiva del Parlamento Europeo y del Consejo sobre la conservación de datos tratados en relación con la prestación de servicios públicos de comunicación electrónica y por la que se modifica la Directiva 2002/58/CE [COM(2005) 438 final; en lo sucesivo, «Propuesta de Directiva»], presentada el mismo día, que dio lugar a la adopción de la Directiva 2006/24 sobre la base del artículo 95 CE.
- 12 El considerando 4 de la Directiva 2006/24 indica lo siguiente:
- «El artículo 15, apartado 1, de la Directiva 2002/58/CE fija las condiciones en que los Estados miembros pueden limitar el alcance de los derechos y obligaciones que se establecen en el artículo 5, el artículo 6, el artículo 8, apartados 1 a 4, y el artículo 9 de dicha Directiva. Tales restricciones deben constituir medidas necesarias, apropiadas y proporcionadas en una sociedad democrática para fines específicos de orden público, como proteger la seguridad nacional (es decir, la seguridad del Estado), la defensa, la seguridad pública, o la prevención, investigación, detección y enjuiciamiento de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas.»
- 13 Según la primera frase del considerando 5 de la citada Directiva, «varios Estados miembros han adoptado legislación que prevé la conservación de datos por los prestadores de servicios para la prevención, investigación, detección y enjuiciamiento de delitos.»
- 14 Los considerandos 7 a 11 de la Directiva 2006/24 están redactados del siguiente modo:

«(7) Las conclusiones del Consejo de Justicia e Interior de 19 de diciembre de 2002 destacan que, a causa del crecimiento significativo de las posibilidades de las comunicaciones electrónicas, los datos relativos al uso de comunicaciones electrónicas son particularmente importantes y, por tanto, una herramienta valiosa en la prevención, investigación, detección y enjuiciamiento de delitos, en especial contra la delincuencia organizada.

(8) La Declaración sobre la lucha contra el terrorismo, adoptada por el Consejo Europeo el 25 de marzo de 2004, encargó al Consejo que examinara medidas para establecer normas sobre la conservación por los prestadores de servicios de datos de tráfico de las comunicaciones.

(9) De conformidad con el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales (CEDH) [firmado en Roma el 4 de noviembre de 1950], toda persona tiene derecho al respeto de su vida privada y de su correspondencia. No podrá haber injerencia de la autoridad pública en el ejercicio de ese derecho salvo cuando esa injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria, entre otras cosas, para la seguridad nacional o la seguridad pública, la prevención de desórdenes o delitos, o la protección de los derechos y las libertades de terceros. Dado que la conservación de datos se ha acreditado como una herramienta de investigación necesaria y eficaz para aplicar la ley en diferentes Estados miembros, en particular en asuntos de gravedad como la delincuencia organizada y el terrorismo, es necesario garantizar que los datos conservados se pongan a disposición de las fuerzas y cuerpos de seguridad durante un determinado período de tiempo, con arreglo a las condiciones establecidas en la presente Directiva. [...]

(10) El 13 de julio de 2005, el Consejo reafirmó en su declaración de condena de los atentados terroristas de Londres la necesidad de adoptar cuanto antes medidas comunes sobre conservación de datos de telecomunicaciones.

(11) Dada la importancia de los datos de tráfico y de localización para la investigación, detección y enjuiciamiento de delitos, según demuestran la investigación y la experiencia práctica de varios Estados miembros, existe la necesidad de asegurar a escala europea que los datos generados o tratados, en el marco de la prestación de servicios de comunicaciones, por proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones se conservan durante un determinado período de tiempo, con arreglo a las condiciones establecidas en la presente Directiva.»

15 Los considerandos 16, 21 y 22 de dicha Directiva señalan lo siguiente:

«(16) Las obligaciones impuestas a los proveedores de servicios en relación con las medidas para garantizar la calidad de los datos, derivadas del artículo 6 de la Directiva 95/46/CE, y sus obligaciones relativas a la garantía de la confidencialidad y seguridad del tratamiento de datos, derivadas de los artículos 16 y 17 de dicha Directiva, son plenamente aplicables a los datos conservados a efectos de la presente Directiva.

[...]

(21) Dado que los objetivos de la presente Directiva, a saber, armonizar las obligaciones de los proveedores de conservar determinados datos y asegurar que éstos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves, tal como se definen en la normativa nacional de cada Estado miembro, como el terrorismo y la delincuencia organizada, no pueden ser alcanzados de manera suficiente por los Estados miembros y, debido a la dimensión y los efectos de la presente Directiva, pueden lograrse mejor a nivel comunitario, la Comunidad puede adoptar medidas, de acuerdo con el principio de subsidiariedad consagrado en el artículo 5 del Tratado. De conformidad con el principio de proporcionalidad enunciado en dicho artículo, la presente Directiva no excede de lo necesario para alcanzar dichos objetivos.

[...]

(22) La presente Directiva respeta los derechos fundamentales y observa los principios reconocidos, en particular, por la Carta de los Derechos Fundamentales de la Unión Europea. En especial, la presente Directiva, junto con la Directiva 2002/58/CE, intenta garantizar el pleno cumplimiento de los derechos fundamentales de los ciudadanos al respeto de la vida privada y de las comunicaciones y a la protección de los datos de carácter personal, consagrados en los artículos 7 y 8 de la Carta.»

- 16 La Directiva 2006/24 establece la obligación de los proveedores de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones de conservar determinados datos generados o tratados por dichos proveedores. A este respecto, los artículos 1 a 9, 11 y 13 de dicha Directiva disponen lo siguiente:

«Artículo 1

Objeto y ámbito

1. La presente Directiva se propone armonizar las disposiciones de los Estados miembros relativas a las obligaciones de los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones en relación con la conservación de determinados datos generados o tratados por los mismos, para garantizar que los datos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves, tal como se definen en la legislación nacional de cada Estado miembro.

2. La presente Directiva se aplicará a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o al usuario registrado. No se aplicará al contenido de las comunicaciones electrónicas, lo que incluye la información consultada utilizando una red de comunicaciones electrónicas.

Artículo 2

Definiciones

1. A efectos de la presente Directiva, se aplicarán las definiciones de la Directiva 95/46/CE, de 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) [...], y de la Directiva 2002/58/CE.
2. A efectos de la presente Directiva, se entenderá por:
 - a) “datos”: los datos de tráfico y de localización y los datos relacionados necesarios para identificar al abonado o usuario;
 - b) “usuario”: toda persona física o jurídica que utilice un servicio de comunicaciones electrónicas de acceso público, con fines privados o comerciales, sin haberse necesariamente abonado a dicho servicio;
 - c) “servicio telefónico”: las llamadas (incluida la transmisión de voz, buzones vocales, conferencias y datos), los servicios suplementarios (incluido el reenvío o transferencia de llamadas) y los servicios de mensajería y servicios multimedia (incluidos los servicios de mensajes cortos, servicios multimedia avanzados y servicios multimedia);
 - d) “identificador de usuario”: un identificador único asignado a las personas con motivo de su abono a un servicio de acceso a Internet o a un servicio de comunicaciones por Internet, o de su registro en uno de dichos servicios;
 - e) “identificador de celda”: la identidad de la celda desde la que se origina o termina una llamada de teléfono móvil;
 - f) “llamada telefónica infructuosa”: una comunicación en el transcurso de la cual se ha realizado con éxito una llamada telefónica pero sin contestación o en la que ha habido una intervención por parte del gestor de la red.

Artículo 3

Obligación de conservar datos

1. Como excepción a los artículos 5, 6 y 9 de la Directiva 2002/58/CE, los Estados miembros adoptarán medidas para garantizar que los datos especificados en el artículo 5 de la presente Directiva se conservan de conformidad con lo dispuesto en ella en la medida en que son generados o tratados por proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones que estén bajo su jurisdicción en el marco de la prestación de los servicios de comunicaciones de que se trate.
2. La obligación de conservar datos mencionada en el apartado 1 incluirá la conservación de los datos especificados en el artículo 5 en relación con las llamadas telefónicas infructuosas en las que los datos los generan o tratan, y conservan (en lo que a los datos telefónicos se refiere) o registran (en lo que a los datos de Internet se refiere), proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones que estén bajo la jurisdicción del Estado miembro de que se trate en el marco de la prestación de los servicios de comunicaciones en cuestión. La conservación de

datos en relación con las llamadas no conectadas no será obligatoria con arreglo a la presente Directiva.

Artículo 4

Acceso a los datos

Los Estados miembros adoptarán medidas para garantizar que los datos conservados de conformidad con la presente Directiva solamente se proporcionen a las autoridades nacionales competentes, en casos específicos y de conformidad con la legislación nacional. Cada Estado miembro definirá en su legislación nacional el procedimiento que deba seguirse y las condiciones que deban cumplirse para tener acceso a los datos conservados de conformidad con los requisitos de necesidad y proporcionalidad, de conformidad con las disposiciones pertinentes del Derecho de la Unión o del Derecho internacional público, y en particular el CEDH en la interpretación del Tribunal Europeo de Derechos Humanos.

Artículo 5

Categorías de datos que deben conservarse

1. Los Estados miembros garantizarán que las siguientes categorías de datos se conserven de conformidad con la presente Directiva:

- a) datos necesarios para rastrear e identificar el origen de una comunicación:
 - 1) con respecto a la telefonía de red fija y a la telefonía móvil:
 - i) el número de teléfono de llamada,
 - ii) el nombre y la dirección del abonado o usuario registrado;
 - 2) con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet:
 - i) la identificación de usuario asignada,
 - ii) la identificación de usuario y el número de teléfono asignados a toda comunicación que acceda a la red pública de telefonía,
 - iii) el nombre y la dirección del abonado o del usuario registrado al que se le ha asignado en el momento de la comunicación una dirección de Protocolo Internet (IP), una identificación de usuario o un número de teléfono;
- b) datos necesarios para identificar el destino de una comunicación:
 - 1) con respecto a la telefonía de red fija y a la telefonía móvil:
 - i) el número o números marcados (el número o números de teléfono de destino) y, en aquellos casos en que intervengan

- otros servicios, como el desvío o la transferencia de llamadas, el número o números hacia los que se transfieren las llamadas,
- ii) los nombres y las direcciones de los abonados o usuarios registrados;
- 2) con respecto al correo electrónico por Internet y a la telefonía por Internet:
- i) la identificación de usuario o el número de teléfono del destinatario o de los destinatarios de una llamada telefónica por Internet,
 - ii) los nombres y direcciones de los abonados o usuarios registrados y la identificación de usuario del destinatario de la comunicación;
- c) datos necesarios para identificar la fecha, hora y duración de una comunicación:
- 1) con respecto a la telefonía de red fija y a la telefonía móvil: la fecha y hora del comienzo y fin de la comunicación,
 - 2) con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet
 - i) la fecha y hora de la conexión y desconexión del servicio de acceso a Internet, basadas en un determinado huso horario, así como la dirección del Protocolo Internet, ya sea dinámica o estática, asignada por el proveedor de acceso a Internet a una comunicación, así como la identificación de usuario del abonado o del usuario registrado,
 - ii) la fecha y hora de la conexión y desconexión del servicio de correo electrónico por Internet o del servicio de telefonía por Internet, basadas en un determinado huso horario;
- d) datos necesarios para identificar el tipo de comunicación:
- 1) con respecto a la telefonía de red fija y a la telefonía móvil: el servicio telefónico utilizado,
 - 2) con respecto al correo electrónico por Internet y a la telefonía por Internet: el servicio de Internet utilizado;
- e) datos necesarios para identificar el equipo de comunicación de los usuarios o lo que se considera ser el equipo de comunicación:
- 1) con respecto a la telefonía de red fija: los números de teléfono de origen y destino,
 - 2) con respecto a la telefonía móvil:

- i) los números de teléfono de origen y destino,
 - ii) la identidad internacional del abonado móvil (IMSI) de la parte que efectúa la llamada,
 - iii) la identidad internacional del equipo móvil (IMEI) de la parte que efectúa la llamada,
 - iv) la IMSI de la parte que recibe la llamada,
 - v) la IMEI de la parte que recibe la llamada,
 - vi) en el caso de los servicios anónimos de pago por adelantado, fecha y hora de la primera activación del servicio y la etiqueta de localización (el identificador de celda) desde la que se haya activado el servicio;
- 3) con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet:
- i) el número de teléfono de origen en caso de acceso mediante marcado de números,
 - ii) la línea digital de abonado (DSL) u otro punto terminal identificador del autor de la comunicación;
- f) datos necesarios para identificar la localización del equipo de comunicación móvil:
- 1) la etiqueta de localización (identificador de celda) al comienzo de la comunicación,
 - 2) los datos que permiten fijar la localización geográfica de la celda, mediante referencia a la etiqueta de localización, durante el período en el que se conservan los datos de las comunicaciones.

2. De conformidad con la presente Directiva, no podrá conservarse ningún dato que revele el contenido de la comunicación.

Artículo 6

Períodos de conservación

Los Estados miembros garantizarán que las categorías de datos mencionadas en el artículo 5 se conserven por un período de tiempo que no sea inferior a seis meses ni superior a dos años a partir de la fecha de la comunicación.

Artículo 7

Protección y seguridad de los datos

Sin perjuicio de lo dispuesto en las disposiciones adoptadas de conformidad con las Directivas 95/46/CE y 2002/58/CE, los Estados miembros velarán por que los

proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones cumplan, en lo que respecta a los datos conservados de conformidad con la presente Directiva, como mínimo los siguientes principios de seguridad de los datos:

- a) los datos conservados serán de la misma calidad y estarán sometidos a las mismas normas de seguridad y protección que los datos existentes en la red;
- b) los datos estarán sujetos a las medidas técnicas y organizativas adecuadas para protegerlos de la destrucción accidental o ilícita, pérdida accidental o alteración, así como almacenamiento, tratamiento, acceso o divulgación no autorizados o ilícitos;
- c) los datos estarán sujetos a medidas técnicas y organizativas apropiadas para velar por que sólo puedan acceder a ellos las personas especialmente autorizadas,

y

- a) los datos, excepto los que hayan sido accesibles y se hayan conservado, se destruirán al término del período de conservación.

Artículo 8

Requisitos de almacenamiento para los datos conservados

Los Estados miembros garantizarán que los datos especificados en el artículo 5 se conservan de conformidad con la presente Directiva de manera que los datos conservados y cualquier otra información necesaria con ellos relacionada puedan transmitirse sin demora cuando las autoridades competentes así lo soliciten.

Artículo 9

Autoridades de control

1. Cada Estado miembro nombrará una o más autoridades públicas responsables de controlar la aplicación en su territorio de las disposiciones adoptadas por los Estados miembros de conformidad con el artículo 7 en relación con la seguridad de los datos conservados. Dichas autoridades podrán ser las mencionadas en el artículo 28 de la Directiva 95/46/CE.

2. Las autoridades mencionadas en el apartado 1 actuarán con plena independencia en el ejercicio del control a que se refiere el apartado 1.

[...]

Artículo 11

Modificación de la Directiva 2002/58/CE

En el artículo 15 de la Directiva 2002/58/CE se inserta el apartado siguiente:

1 bis. El apartado 1 no se aplicará a los datos que deben conservarse específicamente de conformidad con la [Directiva 2006/24] para los fines recogidos en el artículo 1, apartado 1, de dicha Directiva.

[...]

Artículo 13

Recursos judiciales, responsabilidad y sanciones

1. Cada Estado miembro adoptará las medidas que se impongan para velar por que se apliquen plenamente, en lo que se refiere al tratamiento de datos en el marco de la presente Directiva, las medidas nacionales de aplicación del capítulo III de la Directiva 95/46/CE relativas al establecimiento de recursos judiciales, responsabilidad y sanciones.

2. Cada Estado miembro adoptará, en particular, las medidas que se impongan para velar por que cualquier acceso intencionado o la transferencia de datos conservados de conformidad con la presente Directiva que no estén permitidos por la legislación nacional adoptada de conformidad con la presente Directiva se castiguen con sanciones, incluidas sanciones administrativas o penales, que sean eficaces, proporcionadas y disuasorias.»

Litigios principales y cuestiones prejudiciales

Asunto C-293/12

- 17 El 11 de agosto de 2006, Digital Rights interpuso un recurso ante la High Court en el que afirma que es titular de un teléfono móvil que fue registrado el 3 de junio de 2006 y que utiliza desde esa fecha. Cuestiona la legalidad de medidas legislativas y administrativas nacionales sobre la conservación de datos relativos a comunicaciones electrónicas y solicita, en particular, al órgano jurisdiccional remitente que declare la nulidad de la Directiva 2006/24 y de la séptima parte de la Ley de Enjuiciamiento Criminal (Delitos de Terrorismo) de 2005 [Criminal Justice (Terrorist Offences) Act 2005], que establece que los proveedores de servicios de comunicaciones telefónicas deberán conservar los datos de tráfico y localización relativos a esas comunicaciones durante el período establecido en la ley para prevenir y detectar delitos, investigarlos y enjuiciarlos, así como para garantizar la seguridad del Estado.
- 18 Al considerar que no puede pronunciarse sobre las cuestiones que se le plantean sobre la legislación nacional sin que se haya examinado la validez de la Directiva 2006/24, la High Court decidió suspender el procedimiento y plantear al Tribunal de Justicia las siguientes cuestiones prejudiciales:
- «1) ¿Es incompatible la restricción de los derechos del demandante en relación con el uso de telefonía móvil derivada de los requisitos establecidos en los artículos 3, 4, y 6 de la Directiva 2006/24 con el artículo 5 TUE, apartado 4, en la medida en que resulta desproporcionada e innecesaria o inadecuada para lograr los objetivos legítimos de:

- a) garantizar que determinados datos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves
 - y/o
 - b) garantizar el buen funcionamiento del mercado interior de la Unión Europea?
- 2) En particular,
- a) ¿Es compatible la Directiva 2006/24 con el derecho de los ciudadanos a circular y residir libremente en el territorio de los Estados miembros, establecido en el artículo 21 TFUE?
 - b) ¿Es compatible la Directiva 2006/24 con el derecho al respeto de la vida privada establecido en el artículo 7 de la [Carta de los Derechos Fundamentales de la Unión Europea; en lo sucesivo, «Carta»] y en el artículo 8 del [CEDH]?
 - c) ¿Es compatible la Directiva 2006/24 con el derecho a la protección de los datos de carácter personal establecido en el artículo 8 de la Carta?
 - d) ¿Es compatible la Directiva 2006/24 con el derecho a la libertad de expresión establecido en el artículo 11 de la Carta y en el artículo 10 del [CEDH]?
 - e) ¿Es compatible la Directiva 2006/24 con el derecho a una buena administración previsto en el artículo 41 de la Carta?
- 3) ¿En qué medida exigen los Tratados, y en particular el principio de cooperación leal establecido en el artículo 4 TUE, apartado 3, a los órganos jurisdiccionales nacionales indagar y evaluar la compatibilidad de las medidas nacionales de transposición de la Directiva 2006/24 con respecto a las garantías que otorga la [Carta], incluido su artículo 7 (en relación con el artículo 8 del [CEDH])?»

Asunto C-594/12

- 19 La petición de decisión prejudicial en el asunto C-594/12 tiene su origen en varios recursos interpuestos ante el Verfassungsgerichtshof, respectivamente por el Kärntner Landesregierung y los Sres. Seitlinger y Tschohl y otros 11 128 demandantes que solicitan la anulación del artículo 102a de la Ley de telecomunicaciones de 2003 (Telekommunikationsgesetz 2003), que fue introducido por la Ley federal por la que se modifica dicha Ley de telecomunicaciones (Bundesgesetz, mit dem das Telekommunikationsgesetz 2003 — TKG 2003 geändert wird, BGBl. I, 27/2011) con el fin de transponer la Directiva 2006/24 en el ordenamiento jurídico austriaco. Las partes mencionadas consideran, en particular, que el artículo 102a vulnera el derecho fundamental de los particulares a la protección de sus datos.
- 20 El Verfassungsgerichtshof se pregunta concretamente si la Directiva 2006/24 es compatible con la Carta en la medida en que permite que se almacene una masa de

tipos de datos con respecto a un número ilimitado de personas durante un período extenso. Señala que la conservación de datos afecta casi exclusivamente a personas cuyo comportamiento no justifica en modo alguno la conservación de datos referentes a ellas. Según el Verfassungsgerichtshof, estas personas están expuestas al riesgo añadido de que las autoridades investiguen sus datos, conozcan su contenido, se informen sobre su vida privada y utilicen esos datos para múltiples fines, teniendo en cuenta, en particular, el inconmensurable número de personas que tienen acceso a los datos durante un período mínimo de seis meses. El tribunal remitente alberga dudas, por una parte, acerca de si esta Directiva puede lograr los objetivos que persigue y, por otra, sobre el carácter proporcionado de la injerencia en los derechos fundamentales afectados.

21 En estas circunstancias, el Verfassungsgerichtshof decidió suspender el procedimiento y plantear al Tribunal de Justicia las siguientes cuestiones prejudiciales:

«1) Respecto de la validez de actos adoptados por los órganos de la Unión:

¿Son los artículos 3 a 9 de la Directiva 2006/24 compatibles con los artículos 7, 8 y 11 de la [Carta]?

2) Respecto de la interpretación de los Tratados:

a) A la luz de las explicaciones relativas al artículo 8 de la Carta, que, de conformidad con el artículo 52, apartado 7, de la Carta, fueron elaboradas para guiar en la interpretación de [ésta] y deben ser tenidas debidamente en cuenta por el Verfassungsgerichtshof, ¿la Directiva 95/46 y el Reglamento (CE) n° 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos [DO 2001, L 8, p. 11], deben equipararse a los requisitos que recogen los artículos 8, apartado 2, y 52, apartado 1, de la Carta al apreciar la legitimidad de las injerencias?

b) ¿Qué relación guarda el “Derecho de la Unión” a que se refiere la última frase del apartado 3 del artículo 52 de la Carta con las Directivas adoptadas en materia de protección de datos?

c) Dado que la Directiva 95/46 y el Reglamento [...] n° 45/2001 establecen condiciones y límites para el ejercicio del derecho fundamental a la protección de datos, ¿deberán tenerse en cuenta al interpretar el artículo 8 de la Carta las modificaciones a que dé lugar la adopción posterior del Derecho derivado?

d) Teniendo en cuenta el artículo 52, apartado 4, de la Carta, ¿conlleva el principio del nivel más elevado de protección recogido en el artículo 53 de la Carta que deban adoptarse criterios más exigentes que los previstos por [ésta] a la hora de apreciar la legitimidad de las limitaciones establecidas mediante Derecho derivado?

- e) A la vista del artículo 52, apartado 3, de la Carta, del párrafo quinto del Preámbulo de ésta y de las explicaciones relativas al artículo 7 de la misma, en virtud de los cuales los derechos que allí se garantizan corresponden a los que figuran en el artículo 8 del CEDH, ¿pueden emanar de la jurisprudencia del Tribunal Europeo de Derechos Humanos referente al artículo 8 del CEDH criterios que influyan en la interpretación del artículo 8 de la Carta?»

- 22 Mediante auto del Presidente del Tribunal de Justicia de 11 de junio de 2013, se acordó la acumulación de los asuntos C-293/12 y C-594/12 a efectos de la fase oral y de la sentencia.

Sobre las cuestiones prejudiciales

Sobre la segunda cuestión prejudicial, letras b) a d), en el asunto C-293/12 y la primera cuestión prejudicial en el asunto C-594/12

- 23 Mediante la segunda cuestión prejudicial, letras b) a d), en el asunto C-293/12 y la primera cuestión prejudicial en el asunto C-594/12, que procede examinar conjuntamente, los tribunales remitentes solicitan, en definitiva, al Tribunal de Justicia que examine la validez de la Directiva 2006/24 a la luz de los artículos 7, 8 y 11 de la Carta.

Sobre la pertinencia de los artículos 7, 8 y 11 de la Carta en cuanto a la cuestión de la validez de la Directiva 2006/24

- 24 Del artículo 1 y los considerandos 4, 5, 7 a 11, 21 y 22 de la Directiva 2006/24 resulta que el objetivo principal de ésta es armonizar las disposiciones de los Estados miembros relativas a la conservación, por parte de los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones, de determinados datos generados o tratados por dichos proveedores para garantizar que los datos estén disponibles con fines de prevención, investigación, detección y enjuiciamiento de delitos graves, dentro del respeto de los derechos reconocidos en los artículos 7 y 8 de la Carta.

- 25 La obligación de los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones, establecida en el artículo 3 de la Directiva 2006/24, de conservar los datos enumerados en su artículo 5 para que las autoridades nacionales competentes puedan acceder a ellos suscita cuestiones relativas a la protección de la vida privada y de las comunicaciones reconocida en el artículo 7 de la Carta, a la protección de los datos de carácter personal establecida en el artículo 8 de ésta y al respeto de la libertad de expresión garantizada en el artículo 11 de la Carta.

- 26 A este respecto, ha de señalarse que los datos que deben conservar los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones, con arreglo a los artículos 3 y 5 de la Directiva 2006/24, son, en particular, los datos necesarios para rastrear e identificar el origen de una comunicación y su destino, para identificar la fecha, hora y duración de una comunicación, el equipo de comunicación de los usuarios

y para identificar la localización del equipo de comunicación móvil, datos entre los que figuran el nombre y la dirección del abonado o usuario registrado, los números de teléfono de origen y destino y una dirección IP para los servicios de Internet. Estos datos permiten, en particular, saber con qué persona se ha comunicado un abonado o un usuario registrado y de qué modo, así como determinar el momento de la comunicación y el lugar desde la que ésta se ha producido. Además, permiten conocer la frecuencia de las comunicaciones del abonado o del usuario registrado con determinadas personas durante un período concreto.

- 27 Estos datos, considerados en su conjunto, 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 medios sociales que frecuentan.
- 28 En estas circunstancias, aunque la Directiva 2006/24 no autoriza, como se desprende de sus artículos 1, apartado 2, y 5, apartado 2, la conservación del contenido de la comunicación ni de la información consultada al utilizar una red de comunicaciones electrónicas, no se excluye que la conservación de datos controvertida pueda tener una incidencia en el uso por los abonados o usuarios registrados de los medios de comunicación a que se refiere esta Directiva y, en consecuencia, en el ejercicio por parte de éstos de su libertad de expresión, garantizada en el artículo 11 de la Carta.
- 29 La conservación de datos para su eventual acceso por las autoridades nacionales competentes, según se establece en la Directiva 2006/24, afecta de manera directa y específica a la vida privada y, por tanto, a los derechos que garantiza el artículo 7 de la Carta. Además, el artículo 8 de la Carta también es aplicable a dicha conservación de datos, puesto que constituye un tratamiento de datos de carácter personal en el sentido de ese artículo y debe, por tanto, cumplir necesariamente los requisitos de protección de datos que se derivan de dicho artículo (sentencia Volker und Markus Schecke y Eifert, C-92/09 y C-93/09, EU:C:2010:662, apartado 47).
- 30 Si bien las peticiones de decisión prejudicial formuladas en los presentes asuntos plantean concretamente la cuestión de principio de si los datos de los abonados y usuarios inscritos pueden o no conservarse con arreglo al artículo 7 de la Carta, también se refieren a la cuestión de si la Directiva 2006/24 responde a las exigencias de protección de los datos de carácter personal que se derivan del artículo 8 de la Carta.
- 31 En vista de las consideraciones anteriores, para responder a la segunda cuestión prejudicial, letras b) a d), en el asunto C-293/12 y a la primera cuestión prejudicial en el asunto C-594/12, procede examinar la validez de la Directiva a la luz de los artículos 7 y 8 de la Carta.

Sobre la existencia de una injerencia en los derechos reconocidos por los artículos 7 y 8 de la Carta

- 32 Al imponer la conservación de los datos que se indican en el artículo 5, apartado 1, de la Directiva 2006/24 y al permitir el acceso de las autoridades nacionales competentes a éstos, la Directiva establece, como señaló el Abogado General en los puntos 39 y 40 de sus conclusiones, una excepción al régimen de protección del derecho al respeto de la vida privada, establecido por las Directivas 95/46 y 2002/58, con respecto al tratamiento de los datos de carácter personal en el sector de las comunicaciones electrónicas, ya que esas Directivas establecieron la confidencialidad de las comunicaciones y de los datos de tráfico, así como la obligación de borrar o hacer anónimos estos datos cuando ya no son necesarios para la transmisión de una comunicación, salvo si son necesarios para la facturación y únicamente mientras exista esa necesidad.
- 33 Para demostrar la existencia de una injerencia en el derecho fundamental al respeto de la vida privada, carece de relevancia que la información relativa a la vida privada de que se trate tenga o no carácter sensible o que los interesados hayan sufrido o no inconvenientes en razón de tal injerencia (véase, en este sentido, la sentencia *Österreichischer Rundfunk* y otros, C-465/00, C-138/01 y C-139/01, EU:C:2003:294, apartado 75).
- 34 De ello se deduce que la obligación impuesta por los artículos 3 y 6 de la Directiva 2006/24 a los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones de conservar durante un determinado período datos relativos a la vida privada de una persona y a sus comunicaciones, como los que se indican en el artículo 5 de dicha Directiva, constituye en sí misma una injerencia en los derechos garantizados por el artículo 7 de la Carta.
- 35 Además, el acceso de las autoridades nacionales competentes a los datos constituye una injerencia adicional en ese derecho fundamental (véase, en lo que respecta al artículo 8 del CEDH, las sentencias *TEDH, Leander* y *Suecia* de 26 de marzo de 1987, serie A n°116, § 48; *Rotaru c. Rumanía* [GS], n° 28341/95, § 46, CEDH 2000-V, y *Weber y Saravia c. Alemania* (dic.), n° 54934/00, § 79, CEDH 2006-XI). Por lo tanto, los artículos 4 y 8 de la Directiva 2006/24, que establecen normas relativas al acceso de las autoridades nacionales competentes a los datos, también constituyen una injerencia en los derechos garantizados por el artículo 7 de la Carta.
- 36 Asimismo, la Directiva 2006/24 constituye una injerencia en el derecho fundamental a la protección de datos de carácter personal garantizado por el artículo 8 de la Carta puesto que establece un tratamiento de datos de carácter personal.
- 37 Ha de señalarse que, como indicó el Abogado General concretamente en los puntos 77 y 80 de sus conclusiones, la injerencia que supone la Directiva 2006/24 en los derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta resulta de gran magnitud y debe considerarse especialmente grave. Además, la circunstancia de que la conservación de los datos y su posterior utilización se efectúen sin que el abonado o el usuario registrado hayan sido informados de ello puede generar en las personas afectadas el sentimiento de que su vida privada es

objeto de una vigilancia constante, como afirmó el Abogado General en los puntos 52 y 72 de sus conclusiones.

Sobre la justificación de la injerencia en los derechos garantizados por los artículos 7 y 8 de la Carta

- 38 Con arreglo al artículo 52, apartado 1, de la Carta, cualquier limitación del ejercicio de los derechos y libertades reconocidos por ésta deberá ser establecida por la ley, respetar su contenido esencial y, dentro del respeto del principio de proporcionalidad, sólo podrán introducirse limitaciones a dichos derechos y libertades cuando 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.
- 39 En lo que atañe al contenido esencial del derecho fundamental al respeto de la vida privada y de los otros derechos reconocidos en el artículo 7 de la Carta, debe señalarse que, aunque la conservación de datos que la Directiva 2006/24 impone constituye una injerencia especialmente grave en dichos derechos, no puede vulnerar dicho contenido puesto que, como se desprende de su artículo 1, apartado 2, la Directiva no permite conocer el contenido de las comunicaciones electrónicas como tal.
- 40 Esta conservación de datos tampoco puede vulnerar el contenido esencial del derecho fundamental a la protección de datos de carácter personal, reconocido en el artículo 8 de la Carta, ya que la Directiva 2006/24 establece, en su artículo 7, una regla relativa a la protección y a la seguridad de los datos según la cual, sin perjuicio de las disposiciones adoptadas con arreglo a las Directivas 95/46 y 2002/58, los proveedores de servicios de comunicaciones electrónicas de acceso público o de redes públicas de telecomunicaciones deben respetar determinados principios de protección y de seguridad de los datos. Con arreglo a dichos principios, los Estados miembros velarán por que se adopten medidas técnicas y organizativas adecuadas contra la destrucción accidental o ilícita de los datos y su pérdida o alteración accidental.
- 41 En cuanto a la cuestión de si dicha injerencia responde a un objetivo de interés general, ha de señalarse que, si bien la Directiva 2006/24 pretende armonizar las disposiciones de los Estados miembros relativas a las obligaciones de dichos proveedores en relación con la conservación de determinados datos generados o tratados por éstos, el objetivo principal de dicha Directiva es, como se desprende de su artículo 1, apartado 1, garantizar que los datos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves, tal como se definen en la legislación nacional de cada Estado miembro. El objetivo principal de la Directiva es, pues, contribuir a la lucha contra la delincuencia grave y, en definitiva, a la seguridad pública.
- 42 De la jurisprudencia del Tribunal de Justicia se desprende que la lucha contra el terrorismo internacional para el mantenimiento de la paz y la seguridad internacionales es un objetivo de interés general de la Unión (véanse, en este sentido, las sentencias Kadi y Al Barakaat International Foundation/Consejo y Comisión, C-402/05 P y C-415/05 P, EU:C:2008:461, apartado 363, y Al-

Aqsa/Consejo, C-539/10 P y C-550/10 P, EU:C:2012:711, apartado 130). Lo mismo ocurre en lo que respecta a la lucha contra la delincuencia grave para garantizar la seguridad pública (véase, en este sentido, la sentencia Tsakouridis, C-145/09, EU:C:2010:708, apartados 46 y 47). Por otra parte, en relación con esta cuestión procede señalar que el artículo 6 de la Carta establece el derecho de toda persona no sólo a la libertad, sino también a la seguridad.

- 43 A este respecto, en el considerando 7 de la Directiva 2006/24 se indica que, a causa del crecimiento significativo de las posibilidades de las comunicaciones electrónicas, el Consejo de Justicia e Interior de 19 de diciembre de 2002 consideró que los datos relativos al uso de comunicaciones electrónicas son particularmente importantes y, por tanto, una herramienta valiosa en la prevención de delitos y la lucha contra la delincuencia, en especial la delincuencia organizada.
- 44 Por consiguiente, debe reconocerse que la conservación de datos para su eventual acceso por parte de las autoridades nacionales competentes que impone la Directiva 2006/24 responde efectivamente a un objetivo de interés general.
- 45 En estas circunstancias, ha de comprobarse la proporcionalidad de la injerencia constatada.
- 46 A este respecto, procede recordar que, según jurisprudencia reiterada del Tribunal de Justicia, el principio de proporcionalidad exige que los actos de las instituciones de la Unión sean adecuados para lograr los objetivos legítimos perseguidos por la normativa de que se trate y no rebasen los límites de lo que resulta apropiado y necesario para el logro de dichos objetivos (véanse, en este sentido, las sentencias Afton Chemical, EU:C:2010:419, apartado 45; Volker und Markus Schecke y Eifert, EU:C:2010:662, apartado 74; Nelson y otros, C-581/10 y C-629/10, EU:C:2012:657, apartado 71; Sky Österreich, C-283/11, EU:C:2013:28, apartado 50, y Schaible, C-101/12, EU:C:2013:661, apartado 29).
- 47 En lo que atañe al control jurisdiccional de la observancia de estos requisitos, dado que se trata de injerencias en los derechos fundamentales, el alcance de la facultad de apreciación del legislador de la Unión puede resultar limitado en función de una serie de factores, entre los que figuran, en particular, el ámbito afectado, el carácter del derecho en cuestión garantizado por la Carta, la naturaleza y la gravedad de la injerencia, así como la finalidad de ésta (véase, por analogía, en lo que respecta al artículo 8 del CEDH, TEDH, sentencia S y Marper c. Reino Unido [GS], n^{os} 30562/04 y 30566/04, § 102, CEDH 2008-V).
- 48 En el presente asunto, debido, por una parte, al importante papel que desempeña la protección de los datos de carácter personal en lo que respecta al derecho fundamental al respeto de la vida privada y, por otra parte, a la magnitud y gravedad de la injerencia en este derecho que supone la Directiva 2006/24, la facultad de apreciación de legislador de la Unión resulta reducida, por lo que el control de dicha facultad debe ser estricto.
- 49 Por lo que se refiere a la cuestión de si la conservación de datos es adecuada para lograr el objetivo perseguido por la Directiva 2006/24, ha de señalarse que, debido

a la importancia creciente de los medios de comunicación electrónica, los datos que deben conservarse con arreglo a esta Directiva permiten a las autoridades nacionales competentes para la persecución de delitos disponer de más posibilidades para esclarecer delitos graves y, a este respecto, constituyen por tanto una herramienta útil para las investigaciones penales. En consecuencia, la conservación de tales datos puede considerarse adecuada para lograr el objetivo perseguido por dicha Directiva.

- 50 No pone en entredicho esta apreciación la circunstancia —invocada en particular por los Sres. Tschohl y Seitlinger y por el Gobierno portugués en sus observaciones escritas presentadas al Tribunal de Justicia—, de que existen varias modalidades de comunicaciones electrónicas que no están comprendidas en el ámbito de aplicación de la Directiva 2006/24 o que permiten una comunicación anónima. Si bien es cierto que esta circunstancia puede limitar la idoneidad de la medida de conservación de datos para alcanzar el objetivo perseguido, no puede, sin embargo, hacerla inadecuada, como el Abogado General señaló en el punto 137 de sus conclusiones.
- 51 En cuanto al carácter necesario de la conservación de datos que impone la Directiva 2006/24, ha de señalarse que es cierto que la lucha contra la delincuencia grave, especialmente contra la delincuencia organizada y el terrorismo, 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. Sin embargo, este objetivo de interés general, por fundamental que sea, no puede por sí solo justificar que una medida de conservación como la establecida por la Directiva 2006/24 se considere necesaria a los efectos de dicha lucha.
- 52 En lo que respecta al derecho a la intimidad, la protección de este derecho fundamental exige en cualquier caso, 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 (sentencia IPI, C-473/12, EU:C:2013:715, apartado 39 y jurisprudencia citada).
- 53 A este respecto, debe recordarse que la protección de los datos de carácter personal, que resulta de la obligación expresa establecida en el artículo 8, apartado 1, de la Carta, tiene una importancia especial para el derecho al respeto de la vida privada consagrado en el artículo 7 de ésta.
- 54 Por ello, la normativa de la Unión de que se trate debe establecer reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión y establezcan unas exigencias mínimas de modo que las personas cuyos datos se hayan conservado dispongan de garantías suficientes que permitan proteger de manera eficaz sus datos de carácter personal contra los riesgos de abuso y contra cualquier acceso o utilización ilícitos respecto de tales datos (véanse, por analogía, en lo que respecta al artículo 8 del CEDH, las sentencias TEDH, Liberty y otros c. Reino Unido de 1 de julio de 2008, nº 58243/00, §§ 62 y 63; Rotaru c. Rumanía, antes citada, §§ 57 a 59, y S y Marper c. Reino Unido, antes citada, §§ 99).

- 55 La necesidad de disponer de tales garantías es especialmente importante cuando, como establece la Directiva 2006/24, los datos personales se someten a un tratamiento automático y existe un riesgo elevado de acceso ilícito a dichos datos (véanse, por analogía, en lo que respecta al artículo 8 del CEDH, las sentencias TEDH, S y Marper c. Reino Unido, antes citada, § 103, y M. K. c. Francia de 18 de abril de 2013, nº 19522/09, § 35).
- 56 Por lo que se refiere a la cuestión de si la injerencia que supone la Directiva 2006/24 se limita a lo estrictamente necesario, procede señalar que esta Directiva exige, conforme a su artículo 3 en relación con su artículo 5, apartado 1, la conservación de todos los datos de tráfico relativos a la telefonía fija, la telefonía móvil, el acceso a Internet, el correo electrónico por Internet y la telefonía por Internet. Por lo tanto, es aplicable a todos los medios de comunicación electrónica, cuyo uso está muy extendido y que tienen una importancia creciente en la vida cotidiana de las personas. Además, a tenor de su artículo 3, la Directiva comprende a todos los abonados y usuarios registrados. En consecuencia, constituye una injerencia en los derechos fundamentales de prácticamente toda la población europea.
- 57 A este respecto, ha de señalarse, en primer lugar, que la Directiva 2006/24 abarca de manera generalizada a todas las personas, medios de comunicación electrónica y datos relativos al tráfico sin que se establezca ninguna diferenciación, limitación o excepción en función del objetivo de lucha contra los delitos graves.
- 58 En efecto, por una parte, la Directiva 2006/24 afecta con carácter global a todas las personas que utilizan servicios de comunicaciones electrónicas, sin que las personas cuyos datos se conservan se encuentren, ni siquiera indirectamente, en una situación que pueda dar lugar a acciones penales. Por lo tanto, se aplica incluso a personas respecto de las que no existen indicios que sugieran que su comportamiento puede guardar relación, incluso indirecta o remota, con delitos graves. Además, no establece ninguna excepción, por lo que se aplica también a personas cuyas comunicaciones están sujetas al secreto profesional con arreglo a las normas de la legislación nacional.
- 59 Por otra parte, aun cuando la Directiva pretende contribuir a la lucha contra la delincuencia grave, no exige ninguna relación entre los datos cuya conservación se establece y una amenaza para la seguridad pública y, en particular, la conservación no se limita a datos referentes a un período temporal o zona geográfica determinados o a un círculo de personas concretas que puedan estar implicadas de una manera u otra en un delito grave, ni a personas que por otros motivos podrían contribuir, mediante la conservación de sus datos, a la prevención, detección o enjuiciamiento de delitos graves.
- 60 En segundo lugar, a esta falta general de límites se añade que la Directiva 2006/24 no fija ningún criterio objetivo que permita delimitar el acceso de las autoridades nacionales competentes a los datos y su utilización posterior con fines de prevención, detección o enjuiciamiento de delitos que, debido a la magnitud y la gravedad de la injerencia en los derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta, puedan considerarse suficientemente graves para justificar tal injerencia. Por el contrario, la Directiva 2006/24 se limita a remitir de

manera general, en su artículo 1, apartado 1, a los delitos graves tal como se definen en la legislación nacional de cada Estado miembro.

- 61 Además, en cuanto al acceso de las autoridades nacionales competentes a los datos y su utilización posterior, la Directiva 2006/24 no precisa las condiciones materiales y de procedimiento correspondientes. El artículo 4 de la Directiva, que regula el acceso de dichas autoridades a los datos conservados, no dispone expresamente que el acceso y la utilización posterior de los datos de que se trata deberán limitarse estrictamente a fines de prevención y detección de delitos graves delimitados de forma precisa o al enjuiciamiento de tales delitos, sino que se limita a establecer que cada Estado miembro definirá el procedimiento que deba seguirse y las condiciones que deban cumplirse para tener acceso a los datos conservados de conformidad con los requisitos de necesidad y proporcionalidad.
- 62 En particular, la Directiva 2006/24 no establece ningún criterio objetivo que permita limitar el número de personas que disponen de la autorización de acceso y utilización posterior de los datos conservados a lo estrictamente necesario teniendo en cuenta el objetivo perseguido. En especial, el acceso a los datos conservados por las autoridades nacionales competentes no se supedita a un control previo efectuado, bien por un órgano jurisdiccional, bien por un organismo administrativo autónomo, cuya decisión tenga por objeto limitar el acceso a los datos y su utilización a lo estrictamente necesario para alcanzar el objetivo perseguido y se produzca a raíz de una solicitud motivada de dichas autoridades presentada en el marco de procedimientos de prevención, detección o enjuiciamiento de delitos. Tampoco se ha establecido una obligación concreta de los Estados miembros de que se fijen tales limitaciones.
- 63 En tercer lugar, en lo que atañe al período de conservación de los datos, la Directiva 2006/24 prescribe, en su artículo 6, la conservación de éstos durante un período mínimo de seis meses sin que se establezca ninguna distinción entre las categorías de datos previstas en el artículo 5 de la Directiva en función de su posible utilidad para el objetivo perseguido o de las personas afectadas.
- 64 Además, este período oscila entre seis meses como mínimo y veinticuatro meses como máximo, sin que se precise que la determinación del período de conservación debe basarse en criterios objetivos para garantizar que ésta se limite a lo estrictamente necesario.
- 65 De lo anterior resulta que la Directiva 2006/24 no establece reglas claras y precisas que regulen el alcance de la injerencia en los derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta. Por lo tanto, debe considerarse que esta Directiva constituye una injerencia en los derechos fundamentales de gran magnitud y especial gravedad en el ordenamiento jurídico de la Unión, sin que esta injerencia esté regulada de manera precisa por disposiciones que permitan garantizar que se limita efectivamente a lo estrictamente necesario.
- 66 Asimismo, en lo que respecta a las reglas relativas a la seguridad y a la protección de los datos conservados por los proveedores de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, ha de señalarse que la Directiva 2006/24 no contiene garantías

suficientes, como las que exige el artículo 8 de la Carta, que permitan asegurar una protección eficaz de los datos conservados contra los riesgos de abuso y contra cualquier acceso y utilización ilícitos respecto de tales datos. En efecto, en primer lugar, el artículo 7 de la Directiva 2006/24 no establece reglas específicas y adaptadas a la gran cantidad de datos cuya conservación exige esta Directiva, al carácter sensible de estos datos y al riesgo de acceso ilícito a ellos, reglas que tendrían por objeto, en particular, regular de manera clara y estricta la protección y la seguridad de los datos en cuestión, con el fin de garantizar su plena integridad y confidencialidad. Además, tampoco se ha establecido una obligación concreta de los Estados miembros de que se establezcan tales reglas.

67 En particular, el artículo 7 de la Directiva 2006/24, en relación con los artículos 4, apartado 1, de la Directiva 2002/58 y 17, apartado 1, párrafo segundo, de la Directiva 95/46, no garantiza que dichos proveedores apliquen un nivel especialmente elevado de protección y seguridad a través de medidas técnicas y organizativas, sino que autoriza a dichos proveedores a tener en cuenta consideraciones económicas al determinar el nivel de seguridad que aplican en lo que respecta a los costes de aplicación de las medidas de seguridad. En particular, la Directiva 2006/24 no garantiza la destrucción definitiva de los datos al término de su período de conservación.

68 En segundo lugar, ha de añadirse que dicha Directiva no obliga a que los datos en cuestión se conserven en el territorio de la Unión, por lo que no puede considerarse que el control del cumplimiento de los requisitos de protección y seguridad a los que se ha hecho referencia en los dos apartados anteriores está plenamente garantizado por una autoridad independiente, como se exige expresamente en el artículo 8, apartado 3, de la Carta. Dicho control, efectuado sobre la base del Derecho de la Unión, constituye un elemento esencial del respeto a la protección de las personas en lo que respecta al tratamiento de datos personales (véase, en este sentido, la sentencia Comisión/Austria, C-614/10, EU:C:2012:631, apartado 37).

69 Habida cuenta de todas las consideraciones anteriores, ha de considerarse que, al adoptar la Directiva 2006/24, el legislador de la Unión sobrepasó los límites que exige el respeto del principio de proporcionalidad en relación con los artículos 7, 8 y 52, apartado 1, de la Carta.

70 En estas circunstancias, no procede examinar la validez de la Directiva con respecto al artículo 11 de la Carta.

71 Por consiguiente, procede responder a la segunda cuestión, letras b) a d), en el asunto C-293/12 y a la primera cuestión prejudicial en el asunto C-594/12 que la Directiva 2006/24 es inválida.

Sobre la primera cuestión prejudicial y la segunda cuestión prejudicial, letras a) y e), y sobre la tercera cuestión prejudicial en el asunto C-293/12 y sobre la segunda cuestión prejudicial en el asunto C-594/12

72 De lo declarado en el apartado anterior se deduce que no procede responder a la primera cuestión prejudicial, a la segunda cuestión prejudicial, letras a) y e), y a la

tercera cuestión prejudicial en el asunto C-293/12 ni a la segunda cuestión prejudicial en el asunto C-594/12.

Costas

- 73 Dado que el procedimiento tiene, para las partes del litigio principal, el carácter de un incidente promovido ante los órganos jurisdiccionales remitentes, corresponde a éstos resolver sobre las costas. Los gastos efectuados al presentar observaciones ante el Tribunal de Justicia, distintos de aquellos en que hayan incurrido dichas partes, no pueden ser objeto de reembolso.

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

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, es inválida.

Firmas