BASE DE DATOS DE Norma CEF.-
Referencia: NCJ066241

TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA
Sentencia de 20 de septiembre de 2022
Gran Sala
Asuntos acumulados n.º C-339/20 y C-397/20

SUMARIO:

Mercado único de servicios financieros. Abuso de mercado. Información privilegiada. Facultades de supervisión e investigación. Registros de datos de tráfico de un operador de servicios de comunicaciones electrónicas. Tratamiento de datos personales.
El Tribunal de Justicia declara que:
1) El artículo 12, apartado 2, letras a) y d), de la Directiva 2003/6/CE del Parlamento Europeo y del Consejo, de 28 de enero de 2003, sobre las operaciones con información privilegiada y la manipulación del mercado (abuso del mercado) y el artículo 23, apartado 2, letras g) y h), del Reglamento (UE) n.º 596/2014 del Parlamento Europeo y del Consejo, de 16 de abril de 2014, sobre el abuso del mercado (Reglamento sobre abuso del mercado) y por el que se derogan la Directiva 2003/6/CE del Parlamento Europeo y del Consejo, y las Directivas 2003/124/CE, 2003/125/CE y 2004/72/CE de la Comisión, en relación con 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, e interpretados a la luz de los artículos 7, 8 y 11, así como del artículo 52, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea, deben interpretarse en el sentido de que **se oponen a medidas legislativas que establecen, con carácter preventivo, a efectos de la lucha contra los delitos de abuso de mercado, entre los que se encuentran las operaciones con información privilegiada, una conservación generalizada e indiferenciada de los datos de tráfico durante un año a partir del día de su registro**.
2) El Derecho de la Unión debe interpretarse en el sentido de **que se opone a que un órgano jurisdiccional nacional limite en el tiempo los efectos de una declaración de invalidez** que le corresponde efectuar, en virtud del Derecho nacional, con respecto a disposiciones nacionales que, por un lado, imponen a los operadores de servicios de comunicaciones electrónicas una conservación generalizada e indiferenciada de los datos de tráfico y, por otro lado, permiten la comunicación de esos datos a la autoridad competente en materia financiera, sin autorización previa de un órgano jurisdiccional o de una autoridad administrativa independiente, debido a la incompatibilidad de esas disposiciones con el artículo 15, apartado 1, de la Directiva 2002/58, en su versión modificada por la Directiva 2009/136, interpretado a la luz de la Carta de los Derechos Fundamentales de la Unión Europea. La admisibilidad de las pruebas obtenidas con arreglo a las normas nacionales incompatibles con el Derecho de la Unión se rige, conforme al principio de autonomía procesal de los Estados miembros, por el Derecho nacional, siempre que se respeten, en particular, los principios de equivalencia y de efectividad.

PRECEPTOS:

Directiva 2002/58/CE (Privacidad y comunicaciones electrónicas), arts. 1, 2, 5, 6, 9.1 y 15.1.
Directiva 2003/6/CE (operaciones con información privilegiada y la manipulación del mercado), arts. 11 y 12.
Reglamento (UE) nº 596/2014 (Rgto. sobre abuso de mercado), arts. 1, 3.1.27, 14, 22 y 23.

PONENTE:

Don P. G. Xuereb.

En los asuntos acumulados C-339/20 y C-397/20,

que tienen por objeto sendas peticiones de decisión prejudicial planteadas, con arreglo al artículo 267 TFUE, por la Cour de cassation (Tribunal de Casación, Francia), mediante resoluciones de 1 de abril de 2020, recibidas en el Tribunal de Justicia, respectivamente, el 24 de julio de 2020 y el 20 de agosto de 2020, en los procedimientos penales seguidos contra

VD (C-339/20),

SR (C-397/20),

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), N. Piçarra, la Sra. L. S. Rossi y el Sr. A. Kumin, Jueces;

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

Secretaria: Sra. R. Șereș, administradora;

habiendo considerado los escritos obrantes en autos y celebrada la vista el 14 de septiembre de 2021;

consideradas las observaciones presentadas:

– en nombre de VD, por la Sra. D. Foussard y el Sr. F. Peltier, avocats;

– en nombre de SR, por los Sres. M. Chavannes y P. Spinosi, avocats;

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

– en nombre del Gobierno danés, por las Sras. N. Holst-Christensen, N. Lykkegaard 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 la Sra. M. Browne, el Sr. A. Joyce y la Sra. J. Quaney, en calidad de agentes, asistidos por el Sr. D. Fennelly, BL;

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

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

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

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

– en nombre del Supervisor Europeo de Protección de Datos, por la Sra. A. Buchta, el Sr. M. Guglielmetti, la Sra. C.-A. Mamier y el Sr. D. Nardi, 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, en esencia, la interpretación del artículo 12, apartado 2, letras a) y d), de la Directiva 2003/6/CE del Parlamento Europeo y del Consejo, de 28 de enero de 2003, sobre las operaciones con información privilegiada y la manipulación del mercado (abuso del mercado) (DO 2003, L 96, p. 16), así como del artículo 23, apartado 2, letras g) y h), del Reglamento (UE) n.º 596/2014 del Parlamento Europeo y del Consejo, de 16 de abril de 2014, sobre el abuso de mercado (Reglamento sobre abuso de mercado) y por el que se derogan la Directiva 2003/6/CE del Parlamento Europeo y del Consejo, y las Directivas 2003/124/CE, 2003/125/CE y 2004/72/CE de la Comisión (DO 2014, L 173, p. 1), en relación con 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) (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») e interpretados a la luz de los artículos 7, 8, 11 y 52, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, «Carta»).

2. Dichas peticiones fueron presentadas en el contexto de los procesos penales incoados contra VD y SR por delitos de uso de información privilegiada, encubrimiento de delitos de uso de información privilegiada, complicidad, corrupción y blanqueo.

Marco jurídico

Derecho de la Unión

Directiva 2002/58

3. 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/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO 1995, L 281, p. 31)], la presente Directiva no aborda la protección de los derechos y las libertades fundamentales en relación con las actividades no regidas por el Derecho comunitario. Por lo tanto, no altera el equilibrio actual entre el derecho de las personas a la intimidad y la posibilidad de que disponen los Estados miembros, según se indica en el apartado 1 del artículo 15 de la presente Directiva, de tomar las medidas necesarias para la protección de la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando las actividades tengan relación con asuntos de seguridad del Estado) y la aplicación del Derecho penal. En consecuencia, la presente Directiva no afecta a la capacidad de los Estados miembros para interceptar legalmente las comunicaciones electrónicas o tomar otras medidas, cuando sea necesario, para cualquiera de estos fines y de conformidad con el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, [firmado en Roma el 4 de noviembre de 1950] según la interpretación que se hace de este en las sentencias del Tribunal Europeo de Derechos Humanos. Dichas medidas deberán ser necesarias en una sociedad democrática y rigurosamente proporcionales al fin que se pretende alcanzar y deben estar sujetas, además, a salvaguardias adecuadas, de conformidad con el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales.»

4. El artículo 1 de la Directiva 2002/58, titulado «Ámbito de aplicación y objetivo», dispone:

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

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.»

5. El artículo 2 de dicha Directiva, titulado «Definiciones», dispone en su párrafo segundo, letra b):

«[…] a efectos de la presente Directiva se entenderá por:

[…]

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;».

6. A tenor del artículo 5 de la referida 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.

2. El apartado 1 no se aplicará a las grabaciones legalmente autorizadas de comunicaciones y de los datos de tráfico asociados a ellas cuando se lleven a cabo en el marco de una práctica comercial lícita con el fin de aportar pruebas de una transacción comercial o de cualquier otra comunicación comercial.

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.»

7. 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.

[…]»

8. 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. […]»

9. 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 del [TUE].»

Directiva 2003/6

10. Los considerandos 1, 2, 12, 37, 41 y 44 de la Directiva 2003/6 tienen el siguiente tenor:

«(1) Un auténtico mercado único de servicios financieros es crucial para el crecimiento económico y la creación de empleo en la Comunidad.

(2) Un mercado financiero integrado y eficiente requiere integridad del mercado. El buen funcionamiento de los mercados de valores y la confianza del público en los mercados son requisitos imprescindibles para el crecimiento económico y la riqueza. El abuso del mercado daña la integridad de los mercados financieros y a la confianza del público en los valores y productos derivados.

[…]

(12) El abuso del mercado consiste en operaciones con información privilegiada y manipulación del mercado. El objetivo de la legislación contra las operaciones con información privilegiada es el mismo que el de la legislación contra la manipulación del mercado: garantizar la integridad de los mercados financieros comunitarios y aumentar la confianza de los inversores en dichos mercados. […]

[…]

(37) La eficacia de la supervisión quedará garantizada mediante un conjunto mínimo común de competencias e instrumentos eficaces de los que se debe dotar la autoridad competente de cada Estado miembro. Las empresas del mercado y todos los agentes económicos deben contribuir también, a su respectivo nivel, a la integridad del mercado. […]

[…]

(41) Dado que el objetivo de la acción propuesta, a saber, evitar el abuso del mercado en forma de operaciones con información privilegiada o de manipulación del mercado, no puede alcanzarse de manera suficiente por los Estados miembros y, por consiguiente, puede lograrse mejor, debido a las dimensiones o los efectos de la acción, a nivel comunitario, la Comunidad puede adoptar medidas de acuerdo con el principio de subsidiariedad consagrado en el artículo 5 [TUE]. De conformidad con el principio de proporcionalidad enunciado en dicho artículo, la presente Directiva no excede de lo necesario para alcanzar este objetivo.

(44) La presente Directiva respeta los derechos fundamentales y observa los principios reconocidos, en particular, en la [Carta], especialmente en su artículo 11, y en el artículo 10 del Convenio Europeo [para la Protección] de los Derechos Humanos [y de las Libertades Fundamentales]. […]»

11. El artículo 11 de dicha Directiva dispone lo siguiente:

«Sin perjuicio de las competencias propias de las autoridades judiciales, cada Estado miembro designará a una autoridad administrativa única encargada de garantizar la aplicación de las disposiciones adoptadas de conformidad con la presente Directiva.

[…]»

12. A tenor del artículo 12 de la citada Directiva:

«1. La autoridad competente deberá estar dotada de todas las competencias de supervisión e inspección necesarias para el ejercicio de sus funciones. […]

2. Sin perjuicio de lo dispuesto en el apartado 7 del artículo 6, las competencias mencionadas en el apartado 1 del presente artículo se ejercerán de conformidad con la normativa nacional e incluirán al menos el derecho a:

a) acceder a cualquier documento bajo cualquier forma y recibir una copia del mismo;

[…]

d) solicitar registros existentes sobre tráfico de datos y sobre datos telefónicos;

[…]»

Reglamento n.º 596/2014

13. El Reglamento n.º 596/2009 derogó y sustituyó a la Directiva 2003/6 con efectos a partir del 3 de julio de 2016.

14. Los considerandos 1, 2, 7, 24, 44, 62, 65, 66, 77 y 86 de dicho Reglamento tienen el siguiente tenor:

«(1) La existencia de un auténtico mercado interior de servicios financieros es crucial para el crecimiento económico y la creación de empleo en la Unión.

(2) Un mercado financiero integrado, eficiente y transparente requiere la integridad del mercado. El buen funcionamiento de los mercados de valores y la confianza del público en los mercados son requisitos imprescindibles para el crecimiento económico y la riqueza. El abuso del mercado daña la integridad de los mercados financieros y la confianza del público en los valores y los instrumentos derivados.

[…]

(7) El concepto de abuso de mercado abarca conductas ilegales en los mercados financieros y, a los efectos del presente Reglamento, debe entenderse como la realización de operaciones con información privilegiada, la comunicación ilícita de la misma y la manipulación de mercado. Tales conductas impiden la plena y adecuada transparencia del mercado, que es una condición previa para la negociación por parte de los agentes económicos en unos mercados financieros integrados.

[…]

(24) Cuando una persona física o jurídica que posee información privilegiada adquiere, transmite o cede, o intenta adquirir, transmitir o ceder, por cuenta propia o de terceros, directa o indirectamente, instrumentos financieros a los que se refiere dicha información, ha de suponerse que esa persona ha utilizado dicha información. Esta presunción se entiende sin perjuicio del derecho de defensa. La cuestión de si una persona ha infringido la prohibición de realizar operaciones con información privilegiada o ha intentado realizarlas ha de analizarse teniendo en cuenta el objeto del presente Reglamento, que es proteger la integridad de los mercados financieros y aumentar la confianza de los inversores, lo que, a su vez, se basa en la garantía de que estos estarán en igualdad de condiciones y protegidos contra una utilización indebida de información privilegiada.

[…]

(44) El precio de muchos instrumentos financieros se fija sobre la base de índices de referencia. La manipulación o la tentativa de manipulación de los índices de referencia, incluidos los tipos de interés del mercado interbancario, puede tener graves repercusiones en la confianza de los mercados y dar lugar a pérdidas significativas para los inversores o a distorsiones de la economía real. […]

(62) La eficacia de la supervisión se garantiza con la atribución de un conjunto de competencias, instrumentos y recursos eficaces a la autoridad competente de cada Estado miembro. De este modo, el presente Reglamento prevé, en particular, un conjunto mínimo de competencias en materia de supervisión e investigación que se debe confiar en el Derecho interno a las autoridades competentes de los Estados miembros. Cuando la

legislación nacional así lo requiera, dichas competencias se ejercerán mediante solicitud a las autoridades judiciales competentes. […]

[…]

(65) Los registros existentes sobre tráfico de datos y sobre grabaciones de conversaciones telefónicas de las empresas de servicios de inversión, entidades de crédito y entidades financieras que realizan y documentan la realización de las operaciones, así como los registros existentes sobre tráfico de datos y sobre datos telefónicos de las empresas de telecomunicaciones, constituyen una prueba decisiva, a veces la única, para detectar y probar la existencia de operaciones con información privilegiada y de manipulación de mercado. Los registros existentes sobre tráfico de datos y sobre datos telefónicos pueden servir para determinar la identidad de una persona responsable de la difusión de información falsa o engañosa o que las personas de que se trate han estado en contacto durante un cierto tiempo, o la existencia de una relación entre dos o más personas. Por consiguiente, las autoridades competentes deben poder exigir las grabaciones existentes de conversaciones telefónicas, las comunicaciones electrónicas y los registros de tráfico de datos de que disponga una empresa de servicios de inversión, entidad de crédito o entidad financiera de conformidad con la Directiva 2014/65/UE [del Parlamento Europeo y del Consejo, de 15 de mayo de 2014, relativa a los mercados de instrumentos financieros y por la que se modifican la Directiva 2002/92/CE y la Directiva 2011/61/UE (DO 2014, L 173, p. 349)]. El acceso a los registros de tráfico de datos y datos telefónicos es necesario para probar e investigar posibles operaciones con información privilegiada o manipulación de mercado y, por tanto, para detectar y sancionar el abuso de mercado. Para introducir condiciones de competencia equitativas en la Unión en lo que respecta al acceso a los registros de tráfico de datos y sobre datos telefónicos que mantenga una empresa de telecomunicaciones o a las grabaciones existentes de conversaciones telefónicas y tráfico de datos que mantenga una empresa de servicios de inversión, entidad de crédito o entidad financiera, las autoridades competentes deben poder exigir, de conformidad con la normativa nacional, los registros existentes sobre tráfico de datos y sobre datos telefónicos que mantengan las empresas de telecomunicaciones en la medida en que lo autorice la normativa nacional, y las grabaciones existentes de conversaciones telefónicas así como los registros de tráfico de datos que mantengan las empresas de servicios de inversión en los casos en que haya una sospecha razonable de la existencia de dichos registros relativos al asunto de la inspección o la investigación que puedan ser relevantes para probar un caso de información privilegiada o de manipulación de mercado en infracción del presente Reglamento. El acceso a los registros telefónicos y de tráfico de datos que mantiene una empresa de telecomunicaciones no incluye el acceso al contenido de las comunicaciones telefónicas vocales.

(66) Si bien el presente Reglamento establece una serie de competencias de las que, como mínimo, han de disponer las autoridades competentes, estas competencias deben ejercerse en el marco de un sistema completo de Derecho nacional que garantice el respeto de los derechos fundamentales, incluido el derecho a la privacidad. Para el ejercicio de dichas competencias, que pueden dar lugar a graves injerencias en el derecho al respeto de la vida privada y familiar, el hogar y las comunicaciones, los Estados miembros deben disponer de salvaguardias adecuadas y eficaces contra todo abuso, por ejemplo, cuando proceda, un requisito de autorización previa de las autoridades judiciales del Estado miembro de que se trate. Los Estados miembros deben permitir que las autoridades competentes puedan ejercer dichas competencias invasivas, en la medida necesaria para realizar una investigación correcta de casos graves, cuando no haya medios equivalentes para lograr eficazmente el mismo resultado.

[…]

(77) El presente Reglamento respeta los derechos fundamentales y observa los principios reconocidos en la [Carta]. Por consiguiente, el presente Reglamento debe interpretarse y aplicarse de conformidad con dichos derechos y principios. […]

[…]

(86) Dado que el objetivo del presente Reglamento, a saber, evitar el abuso de mercado a través de operaciones con información privilegiada, la comunicación ilícita de la misma y la manipulación de mercado, no puede ser alcanzado de manera suficiente por los Estados miembros sino que, debido a sus dimensiones y efectos, puede lograrse mejor a escala de la Unión esta puede adoptar medidas, de acuerdo con el principio de subsidiariedad establecido en el artículo 5 [TUE]. De conformidad con el principio de proporcionalidad establecido en el mismo artículo, el presente Reglamento no excede de lo necesario para alcanzar dicho objetivo.»

15. Conforme al artículo 1 del referido Reglamento:

«El presente Reglamento establece un marco normativo común en el ámbito de las operaciones con información privilegiada, la comunicación ilícita de información privilegiada y la manipulación de mercado (abuso de mercado), así como medidas para impedir el abuso de mercado a fin de garantizar la integridad de los mercados financieros de la Unión y reforzar la protección de los inversores y su confianza en esos mercados.»

16. Bajo el título «Definiciones», el artículo 3 de dicho Reglamento dispone, en su apartado 1, punto 27:

«A efectos del presente Reglamento se entenderá por:

[…]

27) "registros de tráfico de datos": los registros del tráfico de datos definidos en el artículo 2, párrafo segundo, letra b), de la Directiva [2002/58].»

17. A tenor del artículo 14 del Reglamento n.º 596/2014, titulado «Prohibición de las operaciones con información privilegiada y de la comunicación ilícita de información privilegiada»:

«Ninguna persona podrá:

a) realizar o intentar realizar operaciones con información privilegiada;
b) recomendar que otra persona realice operaciones con información privilegiada o inducirla a ello, o
c) comunicar ilícitamente información privilegiada.»

18. El artículo 22 del citado Reglamento dispone:

«Sin perjuicio de las competencias de las autoridades judiciales, cada Estado miembro designará una autoridad administrativa única que asumirá las competencias relativas al presente Reglamento. […]»

19. El artículo 23 del referido Reglamento, titulado «Facultades de las autoridades competentes», dispone en sus apartados 2 y 3:

«2. Para el ejercicio de las funciones previstas en el presente Reglamento, se deberá dotar a las autoridades competentes, de conformidad con la legislación nacional, al menos de las siguientes facultades en materia de supervisión e investigación:

a) acceder a cualquier documento y dato bajo cualquier forma, y obtener copia del mismo;

[…]

g) solicitar las grabaciones existentes de conversaciones telefónicas, las comunicaciones electrónicas o los registros de tráfico de datos que mantengan las empresas de servicios de inversión, las entidades de crédito o las entidades financieras;
h) solicitar, en la medida en que lo permita la legislación nacional, los registros existentes sobre tráfico de datos que mantenga una empresa de telecomunicaciones cuando haya una sospecha razonable de que se haya cometido una infracción y cuando dichos registros puedan ser relevantes para la investigación de una infracción del artículo 14, letras a) o b), o del artículo 15;

[…]

3. Los Estados miembros velarán por que se adopten las medidas apropiadas para que las autoridades competentes dispongan de todas las facultades de supervisión e investigación necesarias para el desempeño de sus funciones.

[…]»

Derecho francés

CPCE

20. El code des postes et des communications électroniques (Código de Correos y Comunicaciones Electrónicas; en lo sucesivo, «CPCE»), en su redacción aplicable a los litigios principales, disponía en su artículo L. 34-1:

«I. — El presente artículo se aplicará al tratamiento de datos personales en el contexto de la prestación al público de servicios de comunicaciones electrónicas; en particular, se aplicará a las redes que acogen los dispositivos de recogida de datos y de identificación.

II. — Los operadores de comunicaciones electrónicas y, en particular, las personas cuya actividad consista en ofrecer acceso a servicios de comunicación al público en línea, eliminarán o anonimizarán todos los datos de tráfico, sin perjuicio de lo dispuesto en los apartados III, IV, V y VI.

Quienes presten al público servicios de comunicaciones electrónicas establecerán, en observancia de lo indicado en el párrafo anterior, procedimientos internos para atender las demandas de las autoridades competentes.

Quienes, en virtud de una actividad profesional principal o accesoria, ofrezcan al público una conexión que permita una comunicación en línea a través de un acceso a la red, incluso con carácter gratuito, estarán obligados al cumplimiento de las disposiciones aplicables a los operadores de comunicaciones electrónicas en virtud del presente artículo.

III. — A efectos de la investigación, la comprobación y la persecución de delitos o del incumplimiento de la obligación definida en el artículo L. 336-3 del code de la propriété intellectuelle (Código de la Propiedad Intelectual) o a efectos de la prevención de ataques a los sistemas de tratamiento automatizado de datos previstos y castigados por los artículos 323-1 a 323-3-1 del code pénal (Código Penal), y con el único objetivo de permitir, de ser necesario, la puesta a disposición de la autoridad judicial o de la alta autoridad mencionada en el artículo L. 331-12 del Código de la Propiedad Intelectual o de la autoridad nacional de seguridad de los sistemas de información mencionada en el artículo L. 2321-1 del code de la défense (Código de Defensa), podrán aplazarse durante un período máximo de un año las operaciones dirigidas a eliminar o a anonimizar determinadas categorías de datos técnicos. Mediante decreto consultado al Consejo de Estado, adoptado tras el dictamen de la Comisión Nacional de Informática y Libertades, se precisarán, en los límites marcados en el apartado VI, estas categorías de datos y la duración de su conservación, en función de la actividad de los operadores y de la naturaleza de las comunicaciones, así como las modalidades de indemnización, en su caso, de los sobrecostes identificables y específicos de las prestaciones garantizadas en tal concepto, a solicitud del Estado, por los operadores.

[…]

VI. — Los datos conservados y tratados en las condiciones definidas en los apartados III, IV y V versarán exclusivamente sobre la identificación de los usuarios de los servicios suministrados por los proveedores, sobre las características técnicas de las comunicaciones facilitadas por estos últimos y sobre la localización de los equipos terminales.

No podrán referirse en ningún caso al contenido de las correspondencias intercambiadas o la información consultada, bajo cualquier forma, en el marco de dichas comunicaciones.

La conservación y el tratamiento de tales datos se realizará respetando las disposiciones de la loi n.º 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (Ley n.º 78-17 de 6 de enero de 1978 relativa a la informática, a los ficheros y a las libertades).

Los operadores adoptarán todas las medidas para impedir una utilización de esos datos para fines distintos de los previstos en el presente artículo.»

21. El artículo L. 34-1 del CPCE, en su redacción resultante de la loi n.º 2021-998, du 30 juillet 2021, relative à la prévention d'actes de terrorisme et au renseignement (Ley n.º 2021-998, de 30 de julio de 2021, relativa a la prevención de actos de terrorismo y a los servicios de inteligencia) (JORF de 31 de julio de 2021, texto n.º 1), establece, en sus apartados II *bis* a III *bis*:

«II *bis*. Los operadores de comunicaciones electrónicas estarán obligados a conservar:

1° A efectos de los procesos penales, de la prevención de amenazas contra la seguridad pública y de la salvaguardia de la seguridad nacional, la información relativa a la identidad civil del usuario hasta la expiración de un plazo de cinco años a partir del fin de la validez de su contrato;

2° Para los mismos fines enunciados en el punto 1 del presente apartado II *bis*, cualquier otra información facilitada por el usuario en el momento de la celebración de un contrato o de la creación de una cuenta, así como la información relativa al pago, hasta la expiración de un plazo de un año a partir del fin de la validez de su contrato o de la cancelación de su cuenta;

3° A efectos de la lucha contra la criminalidad y la delincuencia grave, de la prevención de amenazas graves contra la seguridad pública y de la salvaguardia de la seguridad nacional, los datos técnicos que permitan identificar

el origen de la conexión o los relativos a los equipos terminales utilizados, hasta la expiración de un plazo de un año a partir de la conexión o utilización de los equipos terminales.

III. Por motivos relacionados con la salvaguardia de la seguridad nacional, cuando se compruebe que existe una amenaza grave, real o previsible, contra esta última, el Primer Ministro podrá, mediante decreto, ordenar a los operadores de comunicaciones electrónicas que conserven, por un período de un año, determinadas categorías de datos de tráfico, además de los mencionados en el punto 3.º del apartado II *bis*, y de los datos de localización especificados mediante decreto consultado al Conseil d'État (Consejo de Estado, Francia).
La orden del Primer Ministro, cuyo plazo de aplicación no podrá exceder de un año, podrá renovarse si siguen cumpliéndose las condiciones previstas para su adopción. Su expiración no afectará al período de conservación de los datos mencionados en el párrafo primero del presente apartado III.

III *bis*. Los datos conservados por los operadores de conformidad con el presente artículo podrán ser objeto de una orden de conservación rápida por parte de las autoridades que, con arreglo a la Ley, tengan acceso a los datos relativos a comunicaciones electrónicas con fines de prevención y represión de la criminalidad, de la delincuencia grave y de otros incumplimientos graves de las normas cuya observancia deben garantizar, con el fin de acceder a esos datos.»

22. El artículo R. 10-13 del CPCE está redactado en los siguientes términos:

«I. — Con arreglo al artículo L. 34-1, apartado III, los operadores de comunicaciones electrónicas conservarán, con fines de investigación, comprobación y persecución de delitos:
a) la información que permita identificar al usuario;

b) los datos relativos a los equipos terminales de comunicación utilizados;
c) las características técnicas, así como la fecha, hora y duración de cada comunicación;
d) los datos relativos a los servicios complementarios solicitados o utilizados y sus proveedores;
e) los datos que permitan identificar el o los destinatarios de la comunicación.

II. — En el caso de las actividades de telefonía, el operador conservará los datos mencionados en el apartado II y, además, los que permitan identificar el origen y la localización de la comunicación.

III. — Los datos mencionados en el presente artículo se conservarán durante un año desde el día de su registro.

[…]»

LCEN

23. El artículo 6 de la loi n.º 2004-575, du 21 juin 2004, pour la confiance dans l'économie numérique (Ley n.º 2004-575, de 21 de junio de 2004, relativa a la confianza en la economía digital) (JORF de 22 de junio de 2004, p. 11168), en su redacción aplicable a los litigios principales (en lo sucesivo, «LCEN»), establecía:

«I. — 1. Las personas cuya actividad consiste en ofrecer acceso a servicios de comunicación al público en línea informarán a sus abonados de la existencia de medios técnicos que permiten restringir el acceso a determinados servicios o seleccionarlos, y les propondrán, al menos, uno de estos medios.

[…]

2. Las personas físicas o jurídicas que almacenen, incluso con carácter gratuito, para la puesta a disposición del público mediante servicios de comunicación al público en línea, señales, textos, imágenes, sonidos o mensajes de cualquier naturaleza proporcionados por destinatarios de estos servicios no podrán incurrir en responsabilidad civil por las actividades o informaciones almacenadas a petición de un destinatario de estos servicios si no tenían efectivamente conocimiento de su carácter ilícito o de los hechos o circunstancias que revelan dicho carácter o si, desde el momento en que tuvieron conocimiento, actuaron sin demora para retirar estos datos o impedir el acceso a ellos.

[…]

II. — Las personas mencionadas en los puntos 1 y 2 del apartado I mantendrán y conservarán los datos de forma tal que permita la identificación de quien haya contribuido a la creación del contenido o de alguno de los contenidos de los servicios de los que son prestadores.

Estas podrán a disposición de quienes publiquen un servicio de comunicación al público en línea medios técnicos que les permitan cumplir los requisitos de identificación establecidos en el apartado III.

La autoridad judicial podrá requerir a los prestadores mencionados en los puntos 1 y 2 del apartado I que comuniquen los datos mencionados en el párrafo primero.

Las disposiciones de los artículos 226-17, 226-21 y 226-22 del Código Penal serán aplicables al tratamiento de estos datos.

Mediante Decreto consultado al Consejo de Estado, adoptado previo dictamen de la Commission nationale de l'informatique et des libertés (Comisión Nacional de Informática y Libertades, Francia) se definirán los datos mencionados en el párrafo primero y se determinarán la duración y las modalidades de su conservación.

[…]»

CMF

24. El artículo L. 621-10 del code monétaire et financier (Código Monetario y Financiero), en su redacción aplicable a los litigios principales (en lo sucesivo, «CMF»), disponía, en su párrafo primero:

«Cuando sea necesario a efectos de la investigación o la inspección, los investigadores o inspectores podrán solicitar que se les haga entrega de cualquier documento en cualquier soporte. Asimismo, los investigadores podrán solicitar los datos conservados y tratados por los operadores de telecomunicaciones en el marco del artículo L. 34-1 del [CPCE] y los proveedores de servicios mencionados en el artículo 6, apartado I, puntos 1 y 2 de la [LCEN] y recibir una copia de dichos datos.

[…]»

25. Extrayendo las consecuencias de la declaración de inconstitucionalidad de la segunda frase del párrafo primero del artículo L. 621-10 del CMF por parte del Conseil constitutionnel (Consejo Constitucional, Francia) en su resolución de 21 de julio de 2017, el legislador, mediante la loi n.º 2018-898, du 23 octobre 2018, relative à la lutte contre la fraude (Ley n.º 2018-898, de 23 de octubre de 2018, relativa a la lucha contra el fraude) (JORF de 24 de octubre de 2018, texto n.º 1), introdujo el artículo L. 621-10-2 en el CMF, que dispone:

«Para la investigación de los abusos de mercado definidos en el Reglamento [n.º 596/2014], los investigadores podrán solicitar los datos conservados y tratados por los operadores de telecomunicaciones, en las condiciones y con los límites establecidos en el artículo L. 34-1 del [CPCE], y por los proveedores mencionados en los puntos 1 y 2 del apartado I del artículo 6 de la [LCEN].

La comunicación de los datos mencionados en el párrafo primero del presente artículo será objeto de una autorización previa por un controlador de las demandas de datos de conexión.

El controlador de las demandas de datos de conexión será, alternativamente, un miembro del Conseil d'État (Consejo de Estado, actuando como Tribunal Supremo de lo Contencioso-Administrativo, Francia), en activo u honorario, elegido por la assemblée générale du Conseil d'État (Asamblea General del Consejo de Estado) y posteriormente por un magistrado de la Cour de cassation (Tribunal de Casación, Francia), en activo u honorario, elegido por la Asamblea General de dicho Tribunal. Su suplente, procedente del otro órgano jurisdiccional, se designará siguiendo las mismas modalidades. El controlador de las demandas de datos de conexión y su suplente serán elegidos por un período de cuatro años no prorrogable.

[…]

El controlador de las demandas de datos de conexión no podrá recibir ni solicitar instrucciones de la Autorité des marchés financiers (Autoridad de los Mercados Financieros, Francia; en lo sucesivo, "AMF") ni de ninguna otra autoridad en el ejercicio de sus funciones. Estará sometido al secreto profesional en las condiciones previstas en el artículo L. 621-4 del presente Código.

El procedimiento se iniciará mediante solicitud motivada del Secretario General o del Secretario General adjunto de la [AMF]. Esta solicitud contendrá los elementos que pueden justificar su procedencia.

La autorización se incorporará al expediente de la investigación.

Los investigadores utilizarán los datos facilitados por los operadores de telecomunicaciones y los proveedores mencionados en el párrafo primero del presente artículo exclusivamente en el marco de la investigación para la que hayan recibido la autorización.

Los datos de conexión relativos a los hechos objeto de pliegos de cargos por parte del Consejo de la [AMF] se destruirán al término de un plazo de seis meses a partir de la decisión definitiva de la Comisión de Sanciones o de los órganos jurisdiccionales competentes para resolver recursos. En caso de composición administrativa, el plazo de seis meses empezará a contar a partir de la ejecución del acuerdo.

Los datos de conexión relativos a hechos que no hayan sido objeto de un pliego de cargos por parte del Consejo de la [AMF] se destruirán al término del plazo de un mes a partir de la fecha de la decisión del Consejo.

En caso de transmisión del informe de la investigación al Fiscal Financiero de la República o en caso de ejercicio de la acción pública por parte del Fiscal Financiero de la República […], los datos de conexión se enviarán al Fiscal Financiero de la República y no serán conservados por la [AMF].

Las modalidades de aplicación del presente artículo se definirán mediante decreto consultado al Consejo de Estado.»

Litigios principales, cuestiones prejudiciales y procedimiento ante el Tribunal de Justicia

26. Mediante escrito de acusación de 22 de mayo de 2014, se inició una instrucción judicial contra VD y SR, relativa a hechos calificados de delitos de uso de información privilegiada y encubrimiento de delitos de uso de información privilegiada. Posteriormente se amplió esa instrucción, mediante un primer escrito de acusación complementario de 14 de noviembre de 2014, respecto a hechos calificados de delito de complicidad.

27. Los días 23 y 25 de septiembre de 2015, la AMF comunicó al juez de instrucción determinados datos de los que disponía en el marco de una investigación llevada a cabo con arreglo al artículo L. 621-10 del CMF, en particular, datos personales procedentes de llamadas telefónicas efectuadas por VD y SR que los investigadores de la AMF habían recabado, sobre la base del artículo L. 34-1 del CPCE, de los operadores de servicios de comunicaciones electrónicas.

28. A raíz de la denuncia realizada de este modo por la AMF, la instrucción se amplió, mediante tres escritos de acusación complementarios de 29 de septiembre de 2015, 22 de diciembre de 2015 y 23 de noviembre de 2016, bajo la calificación de corrupción y blanqueo de capitales.

29. El 10 de marzo y el 29 de mayo de 2017 VD y SR fueron encausados, respectivamente, por los delitos de uso de información privilegiada y blanqueo de capitales, el primero, y por un delito de uso de información privilegiada el segundo.

30. En la medida en que sus respectivos procesamientos se basaban en los datos de tráfico facilitados por la AMF, VD y SR interpusieron sendos recursos ante la cour d'appel de Paris (Tribunal de Apelación de París, Francia), invocando, en particular, un motivo basado, en esencia, en la infracción del artículo 15, apartado 1, de la Directiva 2002/58, interpretado a la luz de los artículos 7, 8, 11 y 52, apartado 1, de la Carta. Más concretamente, basándose en la jurisprudencia derivada 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), VD y SR impugnaban que dicha autoridad se basara, para recabar dichos datos, en el artículo L. 621-10 del CMF y en el artículo L. 34-1 del CPCE, pese a que dichas disposiciones, por una parte, no eran conformes con el Derecho de la Unión, ya que preveían una conservación generalizada e indiferenciada de los datos de conexión, y por otra parte, no establecían ningún límite a la facultad de los investigadores de la AMF de solicitar los datos conservados.

31. Mediante dos sentencias de la cour d'appel de Paris (Tribunal de Apelación de París) de 20 de diciembre de 2018 y de 7 de marzo de 2019, dicho órgano jurisdiccional desestimó los recursos de VD y SR. De las indicaciones que figuran en las peticiones de decisión prejudicial se desprende que, para desestimar el motivo basado, en esencia, en la infracción del artículo 15, apartado 1, de la Directiva 2002/58, interpretado a la luz de los artículos 7, 8, 11 y 52, apartado 1, de la Carta, los jueces que resolvieron sobre el fondo se basaron, en particular, en el hecho de que el artículo 23, apartado 2, letra h), del Reglamento n.º 596/2014, sobre el abuso de mercado, permite a las autoridades competentes solicitar, en la medida en que lo permita la legislación nacional, los registros existentes sobre datos de tráfico que mantengan los operadores de servicios de comunicaciones electrónicas, cuando existen razones para sospechar que se ha producido una infracción de la prohibición de usar información privilegiada, con arreglo al artículo 14, letras a) y b), de dicho Reglamento y cuando dichos registros puedan ser relevantes para la investigación de dicha infracción.

32. VD y SR interpusieron recurso de casación contra esas sentencias ante el órgano jurisdiccional remitente, invocando un motivo basado en la infracción, en particular, de las disposiciones de la Carta y de la Directiva 2002/58 mencionadas en el apartado anterior.

33. Por lo que respecta al acceso a los datos de conexión, el órgano jurisdiccional remitente se refiere a una resolución del Conseil constitutionnel (Consejo Constitucional) de 21 de julio de 2017, de la que, según dicho órgano, se desprende que el procedimiento de acceso a los datos personales conservados por los investigadores de la AMF, tal como está previsto en el Derecho francés, no es conforme con el derecho al respeto de la vida privada, protegido

por el artículo 2 de la Declaración de los Derechos Humanos y del Ciudadano de 1789, y destaca que, si bien el legislador nacional había reservado a los agentes facultados y sujetos al secreto profesional, la facultad de obtener dichos datos en el marco de una investigación y no les había concedido facultades ejecutivas, no había acompañado no obstante dicho procedimiento de ninguna garantía que permitiera asegurar una conciliación equilibrada entre, por un lado, el derecho al respeto de la vida privada y, por otro, la prevención de las alteraciones del orden público y la búsqueda de los autores de infracciones, de modo que la segunda frase del primer párrafo del artículo L. 621-10 del CMF debía ser declarada contraria a la Constitución francesa.

34. El órgano jurisdiccional remitente señala además, por una parte, que el Conseil constitutionnel (Consejo Constitucional) estimó que, habida cuenta de las consecuencias «manifiestamente excesivas» que podría tener una derogación inmediata de dicha disposición sobre los procedimientos en tramitación, procedía diferir la fecha de dicha derogación al 31 de diciembre de 2018 y, por otra parte, que el legislador nacional, extrayendo las consecuencias de la declaración de inconstitucionalidad del párrafo primero del artículo L. 621-10 del CMF, introdujo en dicho código el artículo L. 621-10-2.

35. El órgano jurisdiccional remitente, tras recordar las consideraciones que se desprenden del apartado 125 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), considera que la nulidad de la segunda frase del párrafo primero del artículo L. 621-10 del CMF, aplicable en el momento de los hechos del litigio principal, no puede resultar de dicha declaración de inconstitucionalidad, habida cuenta del aplazamiento de los efectos de la derogación de dicha disposición. Considera, no obstante, que la facultad de que disponen los investigadores de la AMF en virtud de esa disposición, de obtener datos de conexión sin control previo por parte de un órgano jurisdiccional o de una autoridad administrativa independiente, no es conforme con las exigencias derivadas de los artículos 7, 8 y 11 de la Carta, tal como han sido interpretados por el Tribunal de Justicia.

36. En esas circunstancias, a su juicio, solo se plantea a este respecto la cuestión de la posibilidad de aplazar en el tiempo los efectos de la derogación del artículo L. 621-10 del CMF, aun cuando este no sea conforme con la Carta.

37. Por lo que respecta a la conservación de los datos de conexión, el órgano jurisdiccional remitente indica, en primer lugar, que, aunque el apartado II del artículo L. 34-1 del CPCE establece una obligación de principio, conforme a la cual los operadores de servicios de comunicaciones electrónicas deben eliminar o anonimizar cualquier dato relativo al tráfico, esta obligación viene acompañada, no obstante, de una serie de excepciones, entre ellas la prevista en el apartado III de dicha disposición, «a efectos de la investigación, la comprobación y la persecución de delitos». Según dicho órgano jurisdiccional, para estas necesidades concretas, las operaciones de eliminación o de anonimización de determinados datos se difieren en un año.

38. A este respecto, el referido órgano jurisdiccional precisa que las cinco categorías de datos a las que se refieren, en particular, las condiciones definidas en el apartado III del artículo L. 34-1 del CPCE son las enumeradas en el artículo R. 10-13 del CPCE. Estos datos de conexión se generan o tratan tras una comunicación, y se refieren a las circunstancias de dicha comunicación y a los usuarios del servicio, pero no proporcionan, según señala dicho órgano jurisdiccional, ninguna indicación sobre el contenido de las comunicaciones de que se trata.

39. Seguidamente, tras recordar el apartado 112 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), a tenor del cual el artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta, debe interpretarse en el sentido de que se opone a una normativa nacional que establece, con la finalidad de luchar contra la delincuencia, la 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, el órgano jurisdiccional remitente señala que, en el marco de los litigios principales, la AMF tuvo acceso a los datos conservados por los operadores de servicios de comunicaciones electrónicas debido a sospechas relativas a operaciones con información privilegiada y de abuso de mercado que podían tipificarse como diferentes delitos graves. En opinión de dicho órgano jurisdiccional, ese acceso se justificaba por la necesidad de dicha autoridad, a fin de garantizar la eficacia de su investigación, de cruzar diferentes datos conservados a lo largo de un período de tiempo determinado, con el fin de actualizar la información privilegiada que circulaba entre varios interlocutores, lo que reveló la existencia de prácticas ilícitas en la materia.

40. Según el órgano jurisdiccional remitente, las investigaciones llevadas a cabo por la AMF cumplen las obligaciones impuestas a los Estados miembros por el artículo 12, apartado 2, letra d), de la Directiva 2003/6 y por el artículo 23, apartado 2, letras g) y h), del Reglamento n.º 596/2014, en relación con el artículo 1 de dicho

Reglamento, entre ellas, en particular, la obligación de exigir la comunicación de los registros existentes de los datos de tráfico que mantengan los operadores de servicios de comunicaciones electrónicas.

41. Además, dicho órgano jurisdiccional subraya, por un lado, refiriéndose al considerando 65 de dicho Reglamento, que esos datos de conexión constituyen una prueba decisiva, a veces la única, para detectar y probar la existencia de operaciones con información privilegiada, ya que permiten determinar la identidad de una persona responsable de la difusión de información falsa o engañosa, o que las personas de que se trate han estado en contacto durante un cierto tiempo.

42. Por otro lado, el órgano jurisdiccional remitente cita el considerando 66 de este mismo Reglamento, del que se desprende que el ejercicio de las facultades conferidas a las autoridades competentes en materia financiera puede dar lugar a injerencias en el derecho al respeto de la vida privada y familiar, el hogar y de las comunicaciones, y que, por tanto, los Estados miembros deben disponer de salvaguardas adecuadas y eficaces contra todo abuso, limitando dichas facultades únicamente a los casos en que sean necesarias para realizar una investigación correcta de casos graves, cuando no haya medios equivalentes para lograr eficazmente el mismo resultado. En su opinión, de dicho considerando se desprende que determinados casos de abuso de mercado deben considerarse infracciones graves.

43. Por otra parte, dicho órgano jurisdiccional destaca que, en el contexto de los litigios principales, la información privilegiada que podía constituir el elemento material de las prácticas ilícitas en materia de mercado era, por su propia naturaleza, oral y secreta.

44. Habida cuenta de las consideraciones anteriores, el órgano jurisdiccional remitente se pregunta sobre la conciliación del artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta, con las exigencias derivadas del artículo 12, apartado 2, letra d), de la Directiva 2003/6 y del artículo 23, apartado 2, letras g) y h), del Reglamento n.º 596/2014.

45. Por último, en el supuesto de que el Tribunal de Justicia considere que la normativa relativa a la conservación de los datos de conexión controvertida en el litigio principal no es conforme con el Derecho de la Unión, se plantearía la cuestión del mantenimiento provisional de los efectos de dicha normativa, con el fin de evitar la inseguridad jurídica y de permitir que los datos previamente recabados y conservados se utilicen con fines de detección y persecución de las operaciones con información privilegiada.

46. En esas circunstancias, la Cour de cassation (Tribunal de Casación) decidió suspender el procedimiento y plantear al Tribunal de Justicia las siguientes cuestiones prejudiciales, formuladas en términos idénticos en los asuntos C-339/20 y C-397/20:

«1) ¿El artículo 12, apartado 2, letras a) y d), de la Directiva 2003/6 […] y el artículo 23, apartado 2, letras g) y h), del Reglamento [n.º 596/2014], que fue sustituido a partir del 3 de julio de 2016, en relación con el considerando 65 de este mismo Reglamento, no implican, habida cuenta del carácter oculto de la información intercambiada y del gran número de personas susceptibles de ser investigadas, la posibilidad de que el legislador nacional obligue a las empresas de telecomunicaciones electrónicas a conservar con carácter temporal pero de forma generalizada los datos de conexión con el fin de que la autoridad administrativa a que se refieren los artículos 11 de la Directiva [2003/6] y 22 del Reglamento [n.º 596/2014], cuando surgen respecto a determinadas personas motivos para sospechar que están implicadas en una operación con información privilegiada o en una manipulación de mercado, obtenga de la empresa de telecomunicaciones los registros existentes sobre datos de tráfico en casos en los que existan razones para sospechar que dichos registros vinculados al objeto de la investigación pueden ser relevantes para probar la existencia de la infracción, permitiendo, en particular, realizar un seguimiento de los contactos establecidos por los interesados antes de que surgieran las sospechas?

2) En caso de que la respuesta del Tribunal de Justicia […] [a la primera cuestión] conduzca a la Cour de cassation (Tribunal de Casación) a considerar que la normativa francesa relativa a la conservación de los datos de conexión no es compatible con el Derecho de la Unión, ¿pueden mantenerse provisionalmente los efectos de dicha normativa con el fin de evitar la inseguridad jurídica y permitir que los datos recabados y conservados anteriormente sean utilizados en pro de alguno de los objetivos perseguidos por esta normativa?

3) ¿Puede un órgano jurisdiccional nacional mantener provisionalmente los efectos de una normativa que permite a los agentes de una autoridad administrativa independiente encargada de llevar a cabo investigaciones en materia de abuso de mercado obtener la comunicación de datos de conexión sin supeditar esta obtención de datos a un control previo por un órgano jurisdiccional o una autoridad administrativa independiente?»

47. Mediante resolución del Presidente del Tribunal de Justicia de 17 de septiembre de 2020, se acordó la acumulación de los asuntos C-339/20 y C-397/20 a efectos de las fases escrita y oral del procedimiento y de la sentencia.

48. El 21 de abril de 2021, el Conseil d'État (Consejo de Estado, actuando como Tribunal Supremo de lo Contencioso-Administrativo, Francia) dictó la sentencia French Data Network y otros (n.os 393099, 394922, 397844, 397851, 424717 y 424718), en la que se pronunció, en particular, sobre la conformidad con el Derecho de la Unión de determinadas disposiciones legislativas nacionales pertinentes en los litigios principales, a saber, el artículo L. 34-1 del CPCE y el artículo R. 10-13 del CPCE.

49. A instancias del Tribunal de Justicia, los participantes en la vista en los presentes asuntos han tenido la oportunidad de pronunciarse sobre la posible incidencia, para las presentes remisiones prejudiciales, de la mencionada sentencia del Conseil d'État (Consejo de Estado, actuando como Tribunal Supremo de lo Contencioso-Administrativo).

50. El representante del Gobierno francés indicó en esa vista que, mediante la citada sentencia, el Conseil d'État (Consejo de Estado, actuando como Tribunal Supremo de lo Contencioso-Administrativo) declaró ilegales las disposiciones que permiten llevar a cabo la conservación generalizada e indiferenciada de los datos de conexión con el fin de luchar contra la delincuencia, con excepción de la conservación de las direcciones IP y de los datos relativos a la identidad civil de los usuarios de las redes de comunicaciones electrónicas, dando así cumplimiento 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). Precisó, no obstante, que, en el marco del debate contencioso, el Conseil d'État (Consejo de Estado, actuando como Tribunal Supremo de lo Contencioso-Administrativo) debía también dar respuesta a la objeción del Gobierno francés de que esa interpretación del Derecho de la Unión entraba en contradicción con normas de rango constitucional, esto es, las relativas a la prevención de los ataques al orden público, en particular, a la seguridad de las personas y de los bienes, y la búsqueda de los autores de infracciones penales.

51. El representante del Gobierno francés explicó, a este respecto, que el Conseil d'État (Consejo de Estado, actuando como Tribunal Supremo de lo Contencioso-Administrativo) había desestimado en dos fases esta objeción. Por una parte, reconoció ciertamente que la conservación generalizada e indiferenciada de los datos de conexión era una condición determinante del éxito de las investigaciones penales y que ningún otro método podía sustituirlos eficazmente. Por otra parte, no obstante, según el representante del Gobierno francés, el referido Tribunal declaró, apoyándose, en particular, en el apartado 164 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 la conservación rápida de los datos está autorizada por el Derecho de la Unión también cuando esa conservación rápida se refiera a datos conservados inicialmente a efectos de la protección de la seguridad nacional.

52. Por otra parte, el representante del Gobierno francés precisó que, a raíz de la sentencia del Conseil d'État (Consejo de Estado, actuando como Tribunal Supremo de lo Contencioso-Administrativo), de 21 de abril de 2021, French Data Network y otros (n.os 393099, 394922, 397844, 397851, 424717 y 424718), el legislador nacional había introducido el apartado III *bis* en el artículo L. 34-1 del CPCE, como se menciona en el apartado 21 de la presente sentencia.

Sobre las cuestiones prejudiciales

Observaciones preliminares

53. En primer lugar, procede recordar que, con posterioridad a la presentación de las peticiones de decisión prejudicial examinadas, el Conseil d'État (Consejo de Estado, actuando como Tribunal Supremo de lo Contencioso-Administrativo) dictó la sentencia de 21 de abril de 2021, French Data Network y otros (n.os 393099, 394922, 397844, 397851, 424717 y 424718), relativa, en particular, a la compatibilidad con el Derecho de la Unión del artículo L. 34-1 del CPCE y del artículo R. 10-13 del CPCE.

54. Pues bien, como ha señalado el Abogado General en el punto 42 de sus conclusiones, y como se desprende igualmente de las explicaciones facilitadas por el órgano jurisdiccional remitente, recogidas en los apartados 27, 37 y 38 de la presente sentencia, estos artículos constituyen «disposiciones clave» en el contexto de la aplicación del artículo L. 621-10 del CMF, que es objeto de controversia en los litigios principales.

55. En la vista ante el Tribunal de Justicia, el representante del Gobierno francés, tras haber puesto de relieve la evolución legislativa de la que fue objeto el artículo L. 34-1 del CPCE a raíz de las precisiones aportadas

por el Tribunal de Justicia 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), tal como se menciona en el apartado 21 de la presente sentencia, indicó, en esencia, que, para resolver los litigios principales, el órgano jurisdiccional remitente se vería obligado, de conformidad con el principio de aplicación de la Ley en el tiempo consagrado en los artículos 7 y 8 de la Declaración de los Derechos del Hombre y del Ciudadano de 1789, a tomar en consideración las disposiciones nacionales en su redacción aplicable a los hechos controvertidos en el litigio principal, que se remontan a los años 2014 y 2015, de modo que —a su juicio— la sentencia del Conseil d'État (Consejo de Estado, actuando como Tribunal Supremo de lo Contencioso-Administrativo), de 21 de abril de 2021, French Data Network y otros (nos 393099, 394922, 397844, 397851, 424717 y 424718), no puede, en todo caso, ser tomada en consideración al examinar las presentes peticiones de decisión prejudicial.

56. Procede recordar que, según reiterada jurisprudencia, en el marco del procedimiento establecido por el artículo 267 TFUE, corresponde exclusivamente al órgano jurisdiccional nacional, que conoce del litigio y que debe asumir la responsabilidad de la decisión jurisdiccional que debe adoptarse, apreciar, a la luz de las particularidades del asunto, tanto la necesidad de una decisión prejudicial para poder dictar sentencia, como la pertinencia de las cuestiones que plantea al Tribunal de Justicia. Por consiguiente, cuando las cuestiones planteadas se refieran a la interpretación del Derecho de la Unión, el Tribunal de Justicia está, en principio, obligado a pronunciarse (véase, en este sentido, la sentencia de 8 de septiembre de 2010, Winner Wetten, C-409/06, EU:C:2010:503, apartado 36 y jurisprudencia citada).

57. La negativa a pronunciarse sobre una cuestión prejudicial planteada por un órgano jurisdiccional nacional solo es posible cuando resulta evidente que la interpretación del Derecho de la Unión solicitada no tiene relación alguna con la realidad o con el objeto del litigio principal, cuando el problema es de naturaleza hipotética o también cuando el Tribunal de Justicia no dispone de los elementos de hecho o de Derecho necesarios para responder de manera útil a las cuestiones planteadas (véase, en este sentido, la sentencia de 19 de noviembre de 2009, Filipiak, C-314/08, EU:C:2009:719, apartado 42 y jurisprudencia citada).

58. En este caso, de las resoluciones de remisión se desprende que las cuestiones prejudiciales primera y tercera se refieren directamente, no al artículo L. 34-1 del CPCE y al artículo R. 10-13 del CPCE, sino al artículo L. 621-10 del CMF, con arreglo al cual la AMF solicitó a los operadores de servicios de comunicaciones electrónicas la comunicación de los datos de tráfico relativos a llamadas telefónicas efectuadas por VD y SR, sobre cuya base estos últimos fueron investigados y cuya admisibilidad como prueba se cuestiona en el marco de los procedimientos principales.

59. Además, es preciso señalar que, mediante las cuestiones prejudiciales segunda y tercera planteadas en los presentes asuntos, que constituyen una prolongación de las primeras, el órgano jurisdiccional remitente pregunta, en esencia, si, en el supuesto de que la normativa nacional controvertida relativa a la conservación y el acceso a los datos de conexión no sea compatible con el Derecho de la Unión, sus efectos no podrían mantenerse provisionalmente, de modo que se evitara la inseguridad jurídica y se permitiera que los datos conservados sobre la base de dicha normativa pudieran utilizarse con fines de detección y persecución de operaciones con información privilegiada.

60. A la vista de los elementos que preceden, así como de los señalados por el Abogado General en los puntos 44 a 47 de sus conclusiones, procede considerar que, con independencia de la sentencia del Conseil d'État (Consejo de Estado, actuando como Tribunal Supremo de lo Contencioso-Administrativo), de 21 de abril de 2021, French Data Network y otros (n.os 393099, 394922, 397844, 397851, 424717 y 424718), así como de la resolución del Conseil constitutionnel (Consejo Constitucional) de 25 de febrero de 2022 (n.º 2021-976/977), que declaró parcialmente inconstitucional el artículo L. 34-1 del CPCE en la redacción a la que se refiere el apartado 20 de la presente sentencia, sigue siendo necesaria una respuesta del Tribunal de Justicia a las cuestiones prejudiciales para resolver los litigios principales.

61. En segundo lugar, cabe señalar que, en la vista ante el Tribunal de Justicia, el representante de VD cuestionó la aplicabilidad *ratione temporis* del Reglamento n.º 596/2014, alegando, en esencia, que los hechos controvertidos en el litigio principal se produjeron antes de la entrada en vigor de dicho Reglamento. Por tanto, a su juicio, solo las disposiciones de la Directiva 2003/6 son pertinentes a efectos del examen de las cuestiones prejudiciales planteadas por el órgano jurisdiccional remitente.

62. A este respecto, procede recordar que, conforme a reiterada jurisprudencia, una norma jurídica nueva se aplica a partir de la entrada en vigor del acto que la contiene y, si bien no se aplica a las situaciones jurídicas nacidas y definitivamente consolidadas bajo el imperio de la antigua norma, sí se aplica a los efectos futuros de tales

situaciones y a las situaciones jurídicas nuevas. Únicamente deja de ser así, sin perjuicio del principio de irretroactividad de los actos jurídicos, cuando la norma nueva va acompañada de disposiciones particulares que determinan específicamente su ámbito de aplicación temporal. (véanse, en este sentido, las sentencias de 15 de enero de 2019, E. B., C-258/17, EU:C:2019:17, apartado 50 y jurisprudencia citada, y de 14 de mayo de 2020, Azienda Municipale Ambiente C-15/19, EU:C:2020:371, apartado 57).

63. Pues bien, como se ha señalado en los apartados 26 a 29 de la presente sentencia, si bien las situaciones jurídicas de que se trata en los litigios principales surgieron, en efecto, antes de la entrada en vigor del Reglamento n.º 596/2014, que derogó y sustituyó a la Directiva 2003/6 con efectos a partir del 3 de julio de 2016, los procedimientos principales siguieron su curso después de esa fecha, de modo que, a partir de esta, los efectos futuros de esas situaciones se rigen, conforme al principio recordado en el apartado anterior, por el Reglamento n.º 596/2014.

64. De ello se deduce que las disposiciones del Reglamento n.º 596/2014 son aplicables en el caso de autos. Por otra parte, no procede llevar a cabo una distinción entre las disposiciones mencionadas por el órgano jurisdiccional remitente que resultan de la Directiva 2003/6 y del Reglamento n.º 596/2014, ya que estas últimas tienen un alcance esencialmente similar a efectos de la interpretación que el Tribunal de Justicia deberá realizar en el marco de los presentes asuntos.

Sobre las primeras cuestiones prejudiciales

65. Mediante sus primeras cuestiones prejudiciales, el órgano jurisdiccional remitente pregunta, esencialmente, si el artículo 12, apartado 2, letras a) y d), de la Directiva 2003/6 y el artículo 23, apartado 2, letras g) y h), del Reglamento n.º 596/2014, en relación con el artículo 15, apartado 1, de la Directiva 2002/58, e interpretados a la luz de los artículos 7, 8, 11 y 52, apartado 1, de la Carta deben interpretarse en el sentido de que se oponen a medidas legislativas como las controvertidas en los litigios principales que establecen, con carácter preventivo, a efectos de la lucha contra los delitos de abuso de mercado, entre los que se encuentran las operaciones con información privilegiada, una conservación generalizada e indiferenciada de los datos de tráfico durante un año a partir de la fecha de registro.

66. Las partes en los litigios principales y los interesados que han presentado observaciones escritas ante el Tribunal de Justicia han expresado opiniones divergentes a este respecto. Para el Gobierno estonio, Irlanda, así como los Gobiernos español y francés, el artículo 12, apartado 2, letras a) y d), de la Directiva 2003/6 y el artículo 23, apartado 2, letras g) y h), del Reglamento n.º 596/2014 facultan implícita pero necesariamente al legislador nacional a imponer a los operadores de servicios de comunicaciones electrónicas una obligación de conservación generalizada e indiferenciada de datos, con el fin de permitir a la autoridad competente en materia financiera detectar y sancionar las operaciones con información privilegiada. Dado que, como se desprende del considerando 65 del Reglamento n.º 596/2014, tales grabaciones constituyen una prueba decisiva, a veces la única, para detectar y probar la existencia de operaciones con información privilegiada, tal obligación de conservación es, a su juicio, indispensable tanto para garantizar la eficacia de las investigaciones y de las diligencias llevadas a cabo por la referida autoridad, reforzando así el efecto útil del artículo 12, apartado 2, letras a) y d), de la Directiva 2003/6 y del artículo 23, apartado 2, letra h), del Reglamento n.º 596/2014, como para responder a los objetivos de interés general que persiguen dichos instrumentos, que pretenden garantizar la integridad de los mercados financieros de la Unión y reforzar la confianza de los inversores en esos mercados.

67. VD, SR, el Gobierno polaco y la Comisión Europea alegan, en cambio, que esas disposiciones, en la medida en que se limitan a regular la facultad de exigir a los operadores de servicios de comunicaciones electrónicas la comunicación de los registros «existentes» de datos de tráfico que mantengan dichos operadores, solo regulan la cuestión del acceso a esos datos.

68. A este respecto, procede recordar, en primer lugar, que, según reiterada jurisprudencia, para la interpretación de una disposición del Derecho de la Unión, hay que tener en cuenta no solo el tenor de esta, sino también su contexto y los objetivos perseguidos por la normativa de la que forma parte y tomar en consideración, en especial, la génesis de esa normativa (véase, en este sentido, la sentencia de 17 de abril de 2018, Egenberger, C-414/16, EU:C:2018:257, apartado 44).

69. En lo que respecta al tenor de las disposiciones a las que se refieren las primeras cuestiones, procede señalar que, mientras que el artículo 12, apartado 2, letra d), de la Directiva 2003/6 se refiere a la facultad de la autoridad competente en materia financiera de «solicitar registros existentes sobre tráfico de datos y sobre datos telefónicos», el artículo 23, apartado 2, letras g) y h), del Reglamento n.º 596/2014 remite a la facultad de dicha

autoridad de solicitar, por una parte, las «grabaciones […] de tráfico de datos que mantengan las empresas de servicios de inversión, las entidades de crédito o las entidades financieras» y, por otra parte, «en la medida en que lo permita la legislación nacional, los registros existentes sobre tráfico de datos que mantenga una empresa de telecomunicaciones».

70. Pues bien, del tenor de estas disposiciones se desprende inequívocamente que estas se limitan a delimitar la facultad de dicha autoridad de «solicitar» los datos de que disponen esas empresas, lo que corresponde al acceso a esos datos. Además, la referencia hecha a los registros «existentes», que «mantenga» una de dichas empresas, da a entender que el legislador de la Unión no pretendió regular la posibilidad de que el legislador nacional estableciera una obligación de conservación de tales registros.

71. A este respecto, es preciso recordar que, según reiterada jurisprudencia, una interpretación de una disposición del Derecho de la Unión no puede conducir a vaciar de toda eficacia el tenor claro y preciso de esa disposición. Por lo tanto, cuando el sentido de una disposición del Derecho de la Unión se desprende sin ambigüedad de su propio tenor literal, el Tribunal de Justicia no puede apartarse de esta interpretación (sentencia de 25 de enero de 2022, VYSOČINA WIND, C-181/20, EU:C:2022:51, apartado 39 y jurisprudencia citada).

72. La interpretación esbozada en el apartado 70 de la presente sentencia viene corroborada tanto por el contexto en el que se inscriben el artículo 12, apartado 2, letras a) y d), de la Directiva 2003/6 y el artículo 23, apartado 2, letras g) y h), del Reglamento n.º 596/2014 como por los objetivos perseguidos por la normativa de la que forman parte dichas disposiciones.

73. Por lo que respecta al contexto en el que se inscriben esas disposiciones, ha de observarse que, si bien, a tenor del artículo 12, apartado 1, de la Directiva 2003/6 y del artículo 23, apartado 3, del Reglamento n.º 596/2014, interpretado a la luz del considerando 62 de dicho Reglamento, el legislador de la Unión ha querido imponer a los Estados miembros la obligación de adoptar las medidas necesarias para que las autoridades competentes en materia financiera dispongan de un conjunto de herramientas, competencias y recursos adecuados, así como de las facultades de supervisión e investigación necesarias para garantizar la eficacia de sus tareas, esas disposiciones no se pronuncian ni sobre la eventual posibilidad de que los Estados miembros impongan, con ese objetivo, a los operadores de servicios de comunicaciones electrónicas una obligación generalizada e indiferenciada de conservar los datos de tráfico ni sobre las condiciones en las que tales datos deben ser conservados por esos operadores a efectos de entregarlos, en su caso, a las autoridades competentes.

74. Mediante el artículo 12, apartado 2, de la Directiva 2003/6 y el artículo 23, apartado 2, del Reglamento n.º 596/2014, el legislador de la Unión solo pretendió conferir a la autoridad competente en materia financiera, con el fin de garantizar la eficacia de sus tareas de investigación y vigilancia, facultades clásicas de investigación, como las que permiten a dicha autoridad tener acceso a documentos, realizar inspecciones y registros, o también dictar órdenes o prohibiciones contra personas sospechosas de haber cometido infracciones de abuso del mercado, entre las que se encuentran, entre otras, las operaciones con información privilegiada.

75. Por otra parte, es preciso señalar que las disposiciones del Reglamento n.º 596/2014 que regulan específicamente la cuestión de la conservación de datos, a saber, el artículo 11, apartado 5, último párrafo, apartado 6, párrafo segundo, apartado 8, y apartado 11, letra c), el artículo 17, apartado 1, párrafo primero, el artículo 18, apartado 5, y el artículo 28 de dicho Reglamento, solo imponen tal obligación de conservación a los operadores financieros, tal como se enumeran en el artículo 23, apartado 2, letra g), de dicho Reglamento, y se refieren, por tanto, únicamente a los datos correspondientes a transacciones financieras y a servicios prestados por esas empresas concretas.

76. Por lo que respecta a los objetivos perseguidos por la normativa controvertida, cabe observar que, por una parte, de los considerandos 2 y 12 de la Directiva 2003/6 y, por otra parte, del artículo 1 del Reglamento n.º 596/2014, interpretado a la luz de sus considerandos 2 y 24, se desprende que estos instrumentos tienen como finalidad proteger la integridad de los mercados financieros de la Unión y aumentar la confianza de los inversores en esos mercados, confianza que se basa, entre otras cosas, en la garantía de que estarán en igualdad de condiciones y estarán protegidos contra el uso ilícito de información privilegiada. La prohibición de las operaciones con información privilegiada enunciada en el artículo 2, apartado 1, de la Directiva 2003/6 y en el artículo 8, apartado 1, del Reglamento n.º 596/2014 consiste en garantizar la igualdad entre las partes contractuales que intervienen en una operación bursátil, evitando que uno de ellos, poseedor de una información privilegiada que lo sitúa en una posición ventajosa con respecto a los otros inversores, saque provecho de ello en detrimento de la otra parte que desconoce tal información (véase, en este sentido, la sentencia de 15 de marzo de 2022, Autorité des marchés financiers), C-302/20, EU:C:2022/190, apartados 43, 65 y 77 y jurisprudencia citada).

77. Si bien, a tenor del considerando 65 del Reglamento n.º 596/2014, los registros de datos de conexión constituyen una prueba decisiva, a veces la única, para detectar y probar la existencia de operaciones con información privilegiada y de manipulación de mercado, no es menos cierto que dicho considerando solo se refiere a los registros «que mantengan» las empresas de servicios de comunicaciones electrónicas, así como a la facultad de la autoridad competente en materia financiera para «exigir» a esos operadores que comuniquen los datos «existentes». Así pues, de dicho considerando no se desprende en modo alguno que el legislador de la Unión haya querido reconocer a los Estados miembros, mediante dicho Reglamento, la facultad de imponer a los operadores de servicios de comunicaciones electrónicas una obligación general de conservar datos.

78. Habida cuenta de las consideraciones anteriores, procede considerar que ni la Directiva 2003/6 ni el Reglamento n.º 596/2014 pueden interpretarse en el sentido de que constituyen la base jurídica de una obligación general de conservación de los registros de datos de tráfico que mantengan los operadores de servicios de comunicaciones electrónicas a efectos del ejercicio de las facultades conferidas a la autoridad competente en materia financiera en virtud de la Directiva 2003/6 y del Reglamento n.º 596/2014.

79. En segundo lugar, cabe recordar que, como señaló, en esencia, el Abogado General en los puntos 53 y 61 de sus conclusiones, la Directiva 2002/58 constituye el acto de referencia en materia de conservación y, con carácter más general, de tratamiento de datos personales en el sector de las comunicaciones electrónicas, de modo que la interpretación hecha por el Tribunal de Justicia a la luz de esta Directiva regirá también los registros de datos de tráfico que mantengan los operadores de servicios de comunicaciones electrónicas que las autoridades competentes en materia financiera pueden solicitarles, en el sentido del artículo 11 de la Directiva 2003/6 y del artículo 22 del Reglamento n.º 596/2014.

80. En efecto, a tenor del artículo 1, apartado 1, de la Directiva 2002/58, esta prevé, en particular, la armonización de las disposiciones nacionales necesarias para garantizar un nivel equivalente de protección de las libertades y de los derechos fundamentales y, en particular, del derecho a la intimidad y a la confidencialidad, en lo que respecta al tratamiento de los datos personales en el sector de las comunicaciones electrónicas, que engloba también al sector de las telecomunicaciones.

81. Por otra parte, del artículo 3 de la Directiva 2002/58 se desprende que la referida 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 Unión, incluidas las redes públicas de comunicaciones que den soporte a dispositivos de identificación y recopilación de datos. Por lo tanto, debe considerarse que dicha Directiva regula las actividades de los proveedores de tales servicios, entre los que figuran, en particular, los operadores de telecomunicaciones (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 93 y jurisprudencia citada).

82. A la vista de lo anterior, procede considerar que, como alega, en esencia, el Abogado General en los puntos 62 y 63 de sus conclusiones, la apreciación de la licitud del tratamiento de los registros que mantengan los operadores de servicios de comunicaciones electrónicas, en el sentido del artículo 12, apartado 2, letra d), de la Directiva 2003/6 y del artículo 23, apartado 2, letras g) y h), del Reglamento n.º 596/2014, debe efectuarse a la luz de los requisitos establecidos por la Directiva 2002/58 y de la interpretación que de esa Directiva se haga en la jurisprudencia del Tribunal de Justicia.

83. Esta interpretación se ve corroborada por el artículo 3, apartado 1, punto 27, del Reglamento n.º 596/2014, en la medida en que establece que los registros de datos de tráfico a efectos de dicho Reglamento son los definidos en el artículo 2, párrafo segundo, letra b), de la Directiva 2002/58.

84. Además, a tenor del considerando 44 de la Directiva 2003/6 y de los considerandos 66 y 77 del Reglamento n.º 596/2014, las finalidades perseguidas por estos instrumentos deben alcanzarse respetando los derechos fundamentales y los principios consagrados en la Carta, incluido el derecho a la intimidad. A este respecto, el legislador de la Unión indicó expresamente en el considerando 66 del Reglamento n.º 596/2014 que, a efectos del ejercicio de las facultades conferidas a la autoridad competente en materia financiera en virtud de dicho Reglamento, que pueden dar lugar a graves injerencias en el derecho al respeto de la vida privada y familiar, el hogar y las comunicaciones, los Estados miembros deben disponer de salvaguardias adecuadas y eficaces contra todo abuso, por ejemplo, cuando proceda, un requisito de autorización previa de las autoridades judiciales del Estado miembro de que se trate. Los Estados miembros deben permitir que las autoridades competentes puedan ejercer dichas competencias invasivas, en la medida necesaria para realizar una investigación correcta de casos graves, cuando no haya medios equivalentes para lograr eficazmente el mismo resultado. De ello se deduce que la

aplicación de las medidas reguladas por la Directiva 2003/6 y por el Reglamento n.º 596/2014 no puede, en ningún caso, mermar la protección de los datos personales conferida en virtud de la Directiva 2002/58 (véanse, por analogía, las sentencias de 29 de enero de 2008, Promusicae, C-275/06, EU:C:2008:54, apartado 57 y de 17 de junio de 2021, M.I.C.M., C-597/19, EU:C:2021:492, apartado 124 y jurisprudencia citada).

85. Por consiguiente, el artículo 12, apartado 2, letras a) y d), de la Directiva 2003/6 y el artículo 23, apartado 2, letras g) y h), del Reglamento n.º 596/2014 deben interpretarse en el sentido de que no autorizan una conservación generalizada e indiferenciada de los datos de tráfico y de localización a efectos de la lucha contra los delitos de abuso de mercado y, en particular, contra operaciones con información privilegiada, ya que la compatibilidad con el Derecho de la Unión de una normativa nacional que establece tal conservación debe apreciarse sobre la base del artículo 15, apartado 1, de la Directiva 2002/58, interpretado a la luz de los artículos 7, 8, 11 y 52, apartado 1, de la Carta, tal y como lo interpreta la jurisprudencia del Tribunal de Justicia.

86. Por lo que respecta al examen de la compatibilidad de la referida normativa nacional con estas últimas disposiciones, es preciso recordar que, como se desprende, en esencia, de una lectura conjunta de los apartados 53, 54 y 58 de la presente sentencia, si bien la disposición que constituye el núcleo de las presentes remisiones prejudiciales es el artículo L. 621-10 del CMF, en virtud del cual la AMF solicitó a los operadores de servicios de comunicaciones electrónicas la transmisión de los datos de tráfico relativos a llamadas telefónicas efectuadas por VD y SR, sobre cuya base estos últimos fueron encausados, no es menos cierto que, como señaló el Abogado General en el punto 42 de sus conclusiones, el artículo L. 34-1 del CPCE y el artículo R. 10-13 del CPCE constituyen la «clave» en el contexto de la aplicación del mencionado artículo L. 621-10 del CMF.

87. En efecto, de las explicaciones facilitadas por el órgano jurisdiccional remitente, tal como se resumen en los apartados 27, 37 y 38 de la presente sentencia, se desprende, por una parte, que los investigadores de la AMF habían recabado los datos de tráfico de que se trata sobre la base del artículo L. 34-1 del CPCE, en su redacción aplicable a los litigios principales, cuyo apartado III acompañaba la obligación de principio prevista en el apartado II, según la cual los operadores de servicios de comunicaciones electrónicas debían eliminar o anonimizar todos los datos de tráfico, de una serie de excepciones, incluida la relativa a «efectos de la investigación, la comprobación y la persecución de delitos» Para estas necesidades específicas, las operaciones de eliminación o de anonimización de determinados datos se diferían en un año.

88. Por otra parte, dicho órgano jurisdiccional precisa que las cinco categorías de datos a las que se refiere el apartado III del artículo L. 34-1 del CPCE, en su redacción aplicable a los litigios principales, eran las enumeradas en el artículo R. 10-13 del CPCE, a saber, la información que permitía identificar al usuario; los datos relativos a los equipos terminales de comunicación utilizados; las características técnicas, así como la fecha, el horario y la duración de cada comunicación; los datos relativos a los servicios complementarios solicitados o utilizados y sus proveedores y, por último, los datos que permitan identificar al destinatario o destinatarios de la comunicación. Además, del apartado II del artículo R. 10-13 del CPCE, en su redacción aplicable a los litigios principales, se desprende que, para las actividades de telefonía, los operadores afectados también podían conservar los datos que permitieran identificar el origen y la localización de la comunicación.

89. De ello se deduce que la normativa controvertida en el litigio principal abarca todos los medios de comunicaciones telefónicas y engloba a todos los usuarios de esos medios, sin que se establezca una diferenciación o excepción a este respecto. Además, los datos que esta normativa exige conservar a los operadores de servicios de comunicaciones electrónicas son, en particular, los necesarios para rastrear el origen de una comunicación y su destino, determinar la fecha, hora, duración y tipo de comunicación, identificar el material de comunicación utilizado y localizar los equipos terminales y las comunicaciones, datos entre los que figuran, en particular, el nombre y la dirección del usuario, así como los números de teléfono de origen y destino.

90. Así pues, los datos que, en virtud de la normativa nacional controvertida, deben conservarse durante un año, si bien no incluyen el propio contenido de las comunicaciones en cuestión, permiten, entre otras cosas, saber quién es la persona con la que el usuario de un medio de comunicación telefónica ha comunicado y por qué medio tuvo lugar esa comunicación, determinar la fecha, la hora y la duración de las comunicaciones, así como el lugar desde el que tuvieron lugar, y conocer la localización de los equipos terminales sin que se lleve necesariamente a cabo una comunicación. Además, ofrecen la posibilidad de determinar la frecuencia de las comunicaciones del usuario con determinadas personas durante un período concreto. Por tanto, procede concluir que, 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 su 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 (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 45 y jurisprudencia citada).

91. En cuanto a los objetivos perseguidos, procede señalar que la normativa controvertida tiene por objeto, entre otras finalidades, la investigación, la comprobación y la persecución de delitos, incluidos los relativos a los abusos de mercado, entre los que se encuentran las operaciones con información privilegiada.

92. A la vista de lo expuesto en los apartados 86 a 91 de la presente sentencia, procede declarar que, mediante la normativa controvertida, el legislador nacional ha previsto, a efectos, en particular, de la investigación, la comprobación y la persecución de delitos y la lucha contra la delincuencia, una conservación generalizada e indiferenciada de los datos de tráfico durante un año a partir del día del registro.

93. Pues bien, se desprende, en particular, de los apartados 140 a 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), y de los apartados 59 a 101 de la sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros (C-140/20, EU:C:2022:258) que, en virtud del artículo 15, apartado 1, de la Directiva 2002/58, esa conservación no puede justificarse por tales objetivos.

94. De ello resulta que una normativa nacional, como la controvertida en los litigios principales, que obliga a los operadores de servicios de comunicaciones electrónicas a efectuar, con carácter preventivo, a efectos de la lucha contra los delitos de abuso de mercado, entre los que se encuentran las operaciones con información privilegiada, una conservación generalizada e indiferenciada de los datos de tráfico del conjunto de usuarios de medios de comunicación electrónicos, sin que se establezca ninguna diferenciación a este respecto o sin que se establezcan excepciones y sin que queden acreditadas las relaciones necesarias, en virtud de la jurisprudencia mencionada en el apartado anterior, entre los datos que deben conservarse y el objetivo perseguido, excede los límites de lo estrictamente necesario y no puede considerarse justificada en una sociedad democrática, como exige el artículo 15, apartado 1, de la Directiva 2002/58, interpretado a la luz de los artículos 7, 8, 11 y 52, apartado 1, de la Carta (véase, en este sentido, por analogía, la sentencia de 6 de octubre de 2020, Privacy International, C-623/17, EU:C:2020:790, apartado 81).

95. A la vista de todo lo anterior, procede responder a las primeras cuestiones prejudiciales planteadas en los asuntos C-339/20 y C-397/20 que el artículo 12, apartado 2, letras a) y d), de la Directiva 2003/6 y el artículo 23, apartado 2, letras g) y h), del Reglamento n.º 596/2014, en relación con el artículo 15, apartado 1, de la Directiva 2002/58, e interpretados a la luz de los artículos 7, 8, 11 y 52, apartado 1, de la Carta, deben interpretarse en el sentido de que se oponen a medidas legislativas que establecen, con carácter preventivo, a efectos de la lucha contra los delitos de abuso de mercado, entre los que se encuentran las operaciones con información privilegiada, una conservación generalizada e indiferenciada de los datos de tráfico durante un año a partir del día de su registro.

Sobre las cuestiones prejudiciales segunda y tercera

96. Mediante sus cuestiones prejudiciales segunda y tercera planteadas en los presentes asuntos, que procede examinar conjuntamente, el órgano jurisdiccional remitente desea saber, en esencia, si el Derecho de la Unión debe interpretarse en el sentido de que un órgano jurisdiccional nacional puede limitar en el tiempo los efectos de una declaración de invalidez, en virtud del Derecho nacional, con respecto a disposiciones legislativas nacionales que, por un lado, imponen a los operadores de servicios de comunicaciones electrónicas una conservación generalizada e indiferenciada de los datos de tráfico y, por otro lado, permiten la comunicación de esos datos a la autoridad competente en materia financiera, sin autorización previa de un órgano jurisdiccional o de una autoridad administrativa independiente, debido a la incompatibilidad de esa normativa con el artículo 15, apartado 1, de la Directiva 2002/58, interpretado a la luz de la Carta.

97. Cabe recordar de entrada que el principio de primacía del Derecho de la Unión supone la prevalencia de este ordenamiento sobre el Derecho de los Estados miembros. Dicho principio obliga a todos los órganos e instituciones de los Estados miembros, por tanto, a garantizar la plena eficacia de las diferentes disposiciones del Derecho de la Unión, sin que el Derecho de los Estados miembros pueda oponerse al efecto reconocido a las referidas disposiciones en el territorio de estos Estados. En virtud del referido principio, cuando no resulte posible interpretar la normativa nacional conforme a las exigencias del Derecho de la Unión, el juez nacional encargado de aplicar, en el ámbito de su competencia, las disposiciones del Derecho de la Unión tendrá la obligación de garantizar la plena eficacia de estas, dejando inaplicada si fuera necesario, y por su propia iniciativa, cualquier disposición contraria de la legislación nacional, aun posterior, sin que deba solicitar o esperar su previa eliminación por vía

legislativa o mediante cualquier otro procedimiento constitucional (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 118 y jurisprudencia citada).

98. Solo el Tribunal de Justicia puede, con carácter excepcional y en atención a consideraciones imperiosas de seguridad jurídica, suspender provisionalmente el efecto de exclusión que ejerce una norma de la Unión sobre el Derecho nacional contrario a ella. Dicha limitación temporal de los efectos de la interpretación de este Derecho dada por el Tribunal de Justicia solo puede admitirse en la propia sentencia que resuelve sobre la interpretación solicitada. Se estaría actuando en menoscabo de la primacía y de la aplicación uniforme del Derecho de la Unión si los órganos jurisdiccionales nacionales estuvieran facultados para otorgar primacía a las normas nacionales contrarias a este último ordenamiento, aunque fuera con carácter provisional (sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 119 y jurisprudencia citada).

99. Es cierto que el Tribunal de Justicia ha considerado, en un asunto relativo a la legalidad de unas medidas adoptadas incumpliendo la obligación impuesta por el Derecho de la Unión de efectuar una evaluación previa de las repercusiones de un proyecto sobre el medio ambiente y sobre un lugar protegido, que un órgano jurisdiccional nacional puede, si el Derecho interno se lo permite, mantener excepcionalmente los efectos de tales medidas si ese mantenimiento está justificado por consideraciones imperiosas relacionadas con la necesidad de evitar una amenaza real y grave de corte del suministro eléctrico del Estado miembro afectado a la que no podría hacerse frente por otros medios y otras alternativas, en particular en el marco del mercado interior. Dicho mantenimiento solo podrá extenderse el tiempo estrictamente necesario para corregir la referida ilegalidad (véase, en este sentido, la sentencia de 29 de julio de 2019, Inter-Environnement Wallonie y Bond Beter Leefmilieu Vlaanderen, C-411/17, EU:C:2019:622, apartados 175, 176, 179 y 181).

100. Ahora bien, contrariamente al incumplimiento de una obligación procedimental como la evaluación previa de las repercusiones de un proyecto, que se inscribe en el ámbito específico de la protección del medio ambiente, la infracción del 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 puede ser objeto de una regularización mediante un procedimiento comparable al mencionado en el apartado anterior (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 121 y jurisprudencia citada).

101. En efecto, el mantenimiento de los efectos de una normativa nacional como la controvertida en los litigios principales significaría que dicha normativa sigue imponiendo a los operadores de servicios de comunicaciones electrónicas obligaciones que son contrarias al Derecho de la Unión y que suponen injerencias graves en los derechos fundamentales de las personas cuyos datos se han conservado (véase, por analogía, la sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 122 y jurisprudencia citada).

102. Por lo tanto, no le es lícito al órgano jurisdiccional remitente limitar en el tiempo los efectos de una declaración de invalidez que le corresponde efectuar, con arreglo al Derecho nacional, con respecto a la normativa nacional controvertida en los litigios principales (véase, por analogía, la sentencia de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, EU:C:2022:258, apartado 123 y jurisprudencia citada).

103. Debe advertirse, además, que los efectos de la interpretación en cuestión no se limitaron en el tiempo en las sentencias de 21 de diciembre de 2016, Tele2 Sverige y Watson y otros (C-203/15 y C-698/15, EU:C:2016:970), y de 6 de octubre de 2020, La Quadrature du Net y otros (C-511/18, C-512/18 y C-520/18, EU:C:2020:791), de suerte que, conforme a la jurisprudencia recordada en el apartado 98 de la presente sentencia, una sentencia del Tribunal de Justicia posterior a estas sentencias no puede establecer tal limitación.

104. Por último, dado que el órgano jurisdiccional remitente conoce de pretensiones de que se declare la inadmisibilidad de las pruebas obtenidas a partir de los datos de tráfico, basadas en que las disposiciones nacionales controvertidas son contrarias al Derecho de la Unión, tanto en lo que atañe a la conservación de los datos como al acceso a ellos, es preciso determinar la incidencia de la apreciación de la eventual incompatibilidad del artículo L. 621-10 del CMF, en su redacción aplicable a los hechos del litigio principal, con el artículo 15, apartado 1, de la Directiva 2002/58, interpretado a la luz de los artículos 7, 8, 11 y 52, apartado 1, de la Carta, sobre la admisibilidad de las pruebas obtenidas contra VD y SR en el contexto de los litigios principales.

105. A este respecto, basta con remitirse a la jurisprudencia del Tribunal de Justicia, en particular a los principios recordados en los apartados 41 a 44 de la sentencia de 2 de marzo de 2021, Prokuratuur (Condiciones de acceso a los datos relativos a las comunicaciones electrónicas) (C-746/18, EU:C:2021:152), de los que se

desprende que dicha admisibilidad está comprendida, conforme al principio de autonomía procesal de los Estados miembros, en el ámbito del Derecho nacional, siempre que se respeten, en particular, los principios de equivalencia y de efectividad.

106. Por lo que se refiere a este último principio, procede recordar que exige al juez penal nacional que descarte la información y las pruebas que se han obtenido a través de una conservación generalizada e indiferenciada de los datos de tráfico y de localización incompatible con el Derecho de la Unión o incluso mediante el acceso de la autoridad competente a esos datos infringiendo dicho Derecho, en el marco de un proceso penal incoado contra personas sospechosas de haber cometido actos de delincuencia, cuando estas personas no estén en condiciones de comentar eficazmente tal información y tales pruebas, que proceden de un ámbito que escapa al conocimiento de los jueces y que pueden influir destacadamente en la apreciación de los hechos [véase, en este sentido, la sentencia de 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 44 y jurisprudencia citada].

107. Habida cuenta de las consideraciones anteriores, procede responder a las cuestiones prejudiciales segundas y terceras planteadas en los presentes asuntos que el Derecho de la Unión debe interpretarse en el sentido de que se opone a que un órgano jurisdiccional nacional limite en el tiempo los efectos de una declaración de invalidez que le corresponde efectuar, en virtud del Derecho nacional, con respecto a disposiciones nacionales que, por un lado, imponen a los operadores de servicios de comunicaciones electrónicas una conservación generalizada e indiferenciada de los datos de tráfico y, por otro lado, permiten la comunicación de esos datos a la autoridad competente en materia financiera, sin autorización previa de un órgano jurisdiccional o de una autoridad administrativa independiente, debido a la incompatibilidad de esas disposiciones con el artículo 15, apartado 1, de la Directiva 2002/58, interpretado a la luz de la Carta. La admisibilidad de las pruebas obtenidas con arreglo a normas nacionales incompatibles con el Derecho de la Unión se rige, conforme al principio de autonomía procesal de los Estados miembros, por el Derecho nacional, siempre que se respeten, en particular, los principios de equivalencia y de efectividad.

Costas

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

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

1) El artículo 12, apartado 2, letras a) y d), de la Directiva 2003/6/CE del Parlamento Europeo y del Consejo, de 28 de enero de 2003, sobre las operaciones con información privilegiada y la manipulación del mercado (abuso del mercado) y el artículo 23, apartado 2, letras g) y h), del Reglamento (UE) n.º 596/2014 del Parlamento Europeo y del Consejo, de 16 de abril de 2014, sobre el abuso del mercado (Reglamento sobre abuso del mercado) y por el que se derogan la Directiva 2003/6/CE del Parlamento Europeo y del Consejo, y las Directivas 2003/124/CE, 2003/125/CE y 2004/72/CE de la Comisión, en relación con 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, e interpretados a la luz de los artículos 7, 8 y 11, así como del artículo 52, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea,

deben interpretarse en el sentido de que:

se oponen a medidas legislativas que establecen, con carácter preventivo, a efectos de la lucha contra los delitos de abuso de mercado, entre los que se encuentran las operaciones con información privilegiada, una conservación generalizada e indiferenciada de los datos de tráfico durante un año a partir del día de su registro.

2) El Derecho de la Unión debe interpretarse en el sentido de que se opone a que un órgano jurisdiccional nacional limite en el tiempo los efectos de una declaración de invalidez que le corresponde efectuar, en virtud del Derecho nacional, con respecto a disposiciones nacionales que, por un lado, imponen a los operadores de servicios de comunicaciones electrónicas una conservación generalizada e indiferenciada de los datos de tráfico y, por otro lado, permiten la comunicación de esos datos a la autoridad competente en materia financiera, sin autorización previa de un órgano jurisdiccional o de una autoridad

administrativa independiente, debido a la incompatibilidad de esas disposiciones con el artículo 15, apartado 1, de la Directiva 2002/58, en su versión modificada por la Directiva 2009/136, interpretado a la luz de la Carta de los Derechos Fundamentales de la Unión Europea. La admisibilidad de las pruebas obtenidas con arreglo a las normas nacionales incompatibles con el Derecho de la Unión se rige, conforme al principio de autonomía procesal de los Estados miembros, por el Derecho nacional, siempre que se respeten, en particular, los principios de equivalencia y de efectividad.

Firmas

* Lengua de procedimiento: francés.

Fuente: sitio internet del Tribunal de Justicia.