Recopilación de la Jurisprudencia

CONCLUSIONES DEL ABOGADO GENERAL
M. CAMPOS SÁNCHEZ-BORDONA
presentadas el 18 de noviembre de 2021 [1]

Asuntos acumulados C-339/20 y C-397/20

VD (C-339/20)
SR (C-397/20)

[Petición de decisión prejudicial planteada por la Cour de cassation (Tribunal de Casación, Francia)]

«Cuestión prejudicial — Operaciones con información privilegiada y manipulación del mercado — Directiva 2003/6/CE — Artículo 12, apartado 2, letras a) y d) — Reglamento (UE) n.º 596/2014 — Artículo 23, apartado 2, letras g) y h) — Directiva 2002/58/CE — Artículo 15, apartado 1 — Poderes de vigilancia y de investigación de las autoridades competentes — Facultad de las autoridades competentes de exigir los registros telefónicos y de datos intercambiados existentes — Normativa nacional que impone a los operadores de comunicaciones electrónicas una conservación temporal pero generalizada de los datos de conexión»

1. Las peticiones de decisión prejudicial acumuladas en este procedimiento guardan una estrecha relación con las de los asuntos C-793/19, SpaceNet, C-794/19, Telekom Deutschland, y C-140/20, Commissioner of the Garda Síochána y otros, sobre las que también presento mis conclusiones con esta misma fecha. [2]

2. En las conclusiones SpaceNet y Telekom Deutschland y Commissioner of the Garda Síochána expongo las razones que me inducen a sugerir al Tribunal de Justicia una respuesta al Bundesverwaltungsgericht (Tribunal Supremo de lo contencioso administrativo, Alemania) y a la Supreme Court (Tribunal Supremo, Irlanda) en la línea de la jurisprudencia sobre la Directiva 2002/58/CE [3] «recapitulada» en la sentencia La Quadrature du Net. [4]

[1] Lengua original: español.

[2] En lo sucesivo, «conclusiones SpaceNet y Telekom Deutschland» y «conclusiones Commissioner of the Garda Síochána», respectivamente.

[3] Directiva 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).

[4] Sentencia de 6 de octubre de 2020, La Quadrature du Net y otros (C-511/18, C-512/18 y C-520/18, EU:C:2020:791; en lo sucesivo, «sentencia La Quadrature du Net»).

3. Es cierto, sin embargo, que las dos peticiones de decisión prejudicial remitidas por la Cour de Cassation (Tribunal de Casación, Francia) no tienen como objeto inmediato la Directiva 2002/58, sino la Directiva 2003/6/CE [5] y el Reglamento (UE) n.º 596/2014. [6]

4. Ahora bien, lo que en estos dos procedimientos se ventila es, sustancialmente, lo mismo que en aquellos otros reenvíos prejudiciales, a saber, si los Estados miembros pueden imponer la obligación de conservar de manera generalizada e indiferenciada los datos de tráfico de las comunicaciones electrónicas. [7]

5. Por eso, aunque en esta ocasión entren en juego la Directiva 2003/6 y el Reglamento n.º 596/2014 (con los que se pretende combatir las operaciones calificables de abuso del mercado), [8] estimo aplicable en este contexto la jurisprudencia del Tribunal de Justicia condensada en la sentencia La Quadrature du Net.

I. Marco normativo

A. Derecho de la Unión

1. Directiva 2002/58

6. Según el artículo 1 («Ámbito de aplicación y objetivo»):

«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 [Unión].

2. Las disposiciones de la presente Directiva especifican y completan 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)] 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 Tratado de la Unión Europea, 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

[5] Directiva 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).

[6] Reglamento 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 y las Directivas 2003/124/CE, 2003/125/CE y 2004/72/CE de la Comisión (DO 2014, L 173, p. 1).

[7] En este supuesto parecen excluirse los datos de localización, aunque la frontera entre unos y otros no resulta del todo nítida.

[8] En su acepción amplia, que adoptaré en estas conclusiones, el 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» (considerando séptimo del Reglamento n.º 596/2014).

dichas actividades estén relacionadas con la seguridad del mismo) y a las actividades del Estado en materia penal».

7. El artículo 2 («Definiciones») prescribe:

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

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

[…]

b) "datos de tráfico": cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de la facturación de la misma;

c) "datos de localización": cualquier dato tratado en una red de comunicaciones electrónicas o por un servicio de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público;

[…]».

8. El artículo 15 especifica en su apartado 1:

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

2. Directiva 2003/6

9. Con arreglo al artículo 11:

«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.

[…]».

10. A tenor del artículo 12:

«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;

[…]».

3. Reglamento n.º 596/2014

11. El Reglamento contiene estos considerandos:

«(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 de mercado daña la integridad de los mercados financieros y la confianza del público en los valores y los instrumentos derivados.

[…]

(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. 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. […] 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 de los Derechos Fundamentales de la Unión Europea (Carta). Por consiguiente, el presente Reglamento debe interpretarse y aplicarse de conformidad con dichos derechos y principios. […]

[…]».

12. El artículo 1 («Objeto») recoge:

«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».

13. El artículo 3 («Definiciones») señala en su apartado 27 que, a sus efectos, se entenderá por «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 […]».

14. El artículo 22 («Autoridades competentes») prescribe:

«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 […]».

15. El artículo 23 («Facultades de las autoridades competentes») indica:

«[…]

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.

[…]

4. La notificación de información a la autoridad competente con arreglo al presente Reglamento no se considerará infracción de ninguna restricción de comunicación de información impuesta por vía contractual o por cualquier disposición legal, reglamentaria o administrativa, ni implicará para la persona que notifique ningún tipo de responsabilidad en relación con dicha notificación».

16. De acuerdo con el artículo 28 («Protección de datos»):

«En relación con el tratamiento de datos de carácter personal en el marco del presente Reglamento, las autoridades competentes ejercerán las funciones con las que den cumplimiento al presente Reglamento de conformidad con las disposiciones legislativas, reglamentarias o administrativas nacionales de transposición de la Directiva 95/46/CE. En lo que atañe al tratamiento de datos de carácter personal por la [Autoridad Europea de Valores y Mercados (AEVM)]en el marco del presente Reglamento, la AEVM cumplirá con lo dispuesto en el Reglamento (CE) n.º 45/2001 [del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos

personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (DO 2001 L 8, p. 1)].

Los datos de carácter personal se conservarán durante un período máximo de cinco años».

B. Derecho nacional

1. Code monétaire et financier (Código monetario y financiero; en lo sucesivo, «CMF»)

17. El artículo L. 621-10, párrafo primero, del CMF, en la versión vigente en el momento de los hechos, preceptuaba:

«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 code des postes et des communications électroniques (Código de correos y comunicaciones electrónicas; en lo sucesivo «CPCE») y los prestadores de servicios mencionados en el artículo 6, apartado I, puntos 1 y 2 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, de fomento de la confianza en la economía digital [Ley nº 2004-575]) y recibir una copia de dichos datos».

18. Según el artículo L. 621-10-2 del CMF aplicable en el caso:

«Para la investigación de los abusos de mercado […] los investigadores podrán solicitar los datos conservados y tratados por los operadores de telecomunicaciones, en las condiciones y con los límites previstos en el artículo L. 34-1 del [CPCE], y por los prestatarios mencionados en los números 1 y 2 del apartado I del artículo 6 de la [Ley n.º 2004-575].

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.

[…]».

2. CPCE

19. A tenor del artículo L. 34-1 del CPCE vigente en el momento de los hechos:

«[…]

II. Los operadores de comunicaciones electrónicas […] eliminarán o anonimizarán todos los datos de tráfico, sin perjuicio de lo estipulado en los apartados III […]

[…]

III. A efectos de la investigación, la comprobación y la persecución de delitos […] podrán aplazarse durante un período máximo de un año las operaciones dirigidas a eliminar o a anonimizar determinadas categorías de datos técnicos. […]

[…]

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 las informaciones consultadas, bajo cualquier forma, en el marco de dichas comunicaciones.

[…]».

20. El artículo R. 10-13 del CPCE disponía:

«I. Con arreglo al apartado III del artículo L. 34-1, los operadores de comunicaciones electrónicas conservarán, a los fines de la investigación, de la constatación y de la persecución de delitos:

a) las informaciones que permitan identificar al usuario;

b) los datos relativos a los equipos terminales de comunicaciones 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.

[…]».

21. El tribunal de reenvío precisa que tales datos de conexión son aquellos que, generados o tratados como consecuencia de una comunicación, atañen a las circunstancias de esta y a los usuarios del servicio, con exclusión de cualquier indicación sobre el contenido de los mensajes.

II. Hechos, litigios y preguntas prejudiciales

22. Los hechos que están en la base de estos dos reenvíos prejudiciales coinciden en lo sustancial.

23. Mediante un escrito de acusación de 22 de mayo de 2014, se inició una instrucción judicial para investigar actuaciones tipificadas como delitos de uso de información privilegiada y encubrimiento.

24. Los días 23 y 25 de septiembre de 2015, l'Autorité des marchés financiers (Autoridad de los Mercados Financieros; en lo sucesivo, «AMF») envió al Ministerio Fiscal una comunicación a la que adjuntaba documentos procedentes de una investigación, llevada a cabo por ella, que incluían, en particular, datos personales relativos a la utilización de líneas telefónicas.

25. Para recabar los datos relativos a la utilización de esas líneas telefónicas, los agentes de la AMF se basaron en el artículo L. 621-10 del CMF.

26. A raíz de esa comunicación, mediante tres escritos de acusación complementarios de 29 de septiembre, 22 de diciembre de 2015 y 23 de noviembre de 2016, se amplió el objeto de la instrucción para incluir determinados títulos e instrumentos financieros conexos, por los mismos delitos y por hechos tipificados como complicidad delictiva, corrupción y blanqueo de capitales.

27. Acusados de los delitos de uso de información privilegiada y blanqueo de capitales por hechos relacionados con dichos títulos, VD y SR interpusieron recurso de anulación, interesando la exclusión de documentos procesales por infracción, entre otros, de los artículos 7, 8, 11 y 52 de la Carta y del artículo 15 de la Directiva 2002/58.

28. Desestimadas sus pretensiones por sendas sentencias, de 20 de diciembre de 2018 y 7 de marzo de 2019, de la chambre de l'instruction de la cour d'appel de Paris, 2e section (Sala de instrucción del Tribunal de apelación de París, sección 2.ª, Francia), los acusados las recurrieron ante la Cour de cassation (Tribunal de Casación), que eleva al Tribunal de Justicia estas preguntas prejudiciales:

«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 596/2014 […], 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 y 22 del Reglamento, 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 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?»

III. Procedimiento ante el Tribunal de Justicia

29. Las peticiones de decisión prejudicial se registraron en el Tribunal de Justicia, respectivamente, el 24 de julio de 2020 y el 20 de agosto de 2020.

30. Han depositado observaciones escritas VD, SR, los Gobiernos español, estonio, francés, irlandés, polaco y portugués, así como la Comisión Europea.

31. En la vista pública celebrada el 14 de septiembre de 2021 comparecieron VD, SR, los Gobiernos francés, danés, estonio, español e irlandés, la Comisión Europea y el Supervisor Europeo para la Protección de Datos.

IV. Análisis

A. Consideraciones preliminares

32. La normativa nacional relevante en estos dos procedimientos ha sido objeto de determinados pronunciamientos jurisdiccionales internos que es oportuno mencionar.

1. Sentencia del Conseil constitutionnel (Consejo Constitucional, Francia) de 21 de julio de 2017

33. El tribunal de reenvío ha puesto de manifiesto que el párrafo primero del artículo L. 621-10 del CMF fue declarado inconstitucional por sentencia del Conseil constitutionnel (Consejo Constitucional) de 21 de julio de 2017.[9]

34. El Conseil constitutionnel (Consejo Constitucional) pospuso, sin embargo, los efectos de la declaración de inconstitucionalidad al 31 de diciembre de 2018.

35. En el ínterin, el legislador nacional introdujo en el CMF el artículo L. 621-10-2, por el que instauró un régimen de autorización previa, a cargo de una autoridad administrativa independiente, para acceder a los datos de conexión.

36. Según el tribunal de reenvío:

— Dado el aplazamiento de los efectos de la declaración de inconstitucionalidad del párrafo primero del artículo L. 621-10 del CMF —vigente en el momento de los hechos controvertidos en los procesos *a quibus*—, no cabe apreciar la nulidad de dicha disposición;[10]

[9] El Conseil constitutionnel (Consejo Constitucional) habría apreciado la incompatibilidad del procedimiento de acceso de la AMF a los datos de conexión con el derecho al respeto a la vida privada, protegido por el artículo 2 de la Declaración de los Derechos del Hombre y del Ciudadano.

[10] Apartado 28 del auto de reenvío de la cuestión prejudicial C-339/20 y apartado 43 del de la cuestión prejudicial C-397/20.

— no obstante, tal disposición, en la medida en que no supeditaba el acceso a los datos de conexión a un control previo por parte de un órgano jurisdiccional o de una autoridad administrativa independiente, «no era compatible con las exigencias establecidas por los artículos 7, 8 y 11 de la Carta […], tal como los interpreta el [Tribunal de Justicia]». [11]

37. En esa tesitura, la Cour de cassation (Tribunal de Casación) concluye que la «única cuestión que se plantea se refiere a la posibilidad de retrasar los efectos de la incompatibilidad del artículo L. 621-10 del [CMF]». [12]

38. El tribunal de reenvío no pregunta, pues, por la compatibilidad del artículo L. 621-10 del CMF con el derecho de la Unión, sino que, partiendo de su incompatibilidad con varios preceptos de la Carta, solo quiere saber si, al igual que ha sucedido en el derecho interno con los efectos de la declaración de inconstitucionalidad de aquel precepto, es posible también retrasar los efectos jurídicos correspondientes a su disconformidad con el derecho de la Unión. Ese es el objeto de la tercera pregunta prejudicial.

2. Sentencia de 21 de abril de 2021 del Conseil d'État (Consejo de Estado, Francia)

39. Con posterioridad al planteamiento de estas dos peticiones de decisión prejudiciales, el Conseil d'État (Consejo de Estado) dictó sentencia, el 21 de abril de 2021, [13] en el procedimiento durante cuya tramitación se planteó la petición de decisión prejudicial que dio lugar a la sentencia La Quadrature du Net.

40. En esa sentencia, el Conseil d'État (Consejo de Estado) ha resuelto descartar la aplicación del artículo L. 34-1 del CPCE y conminar al Gobierno para que, en el plazo de seis meses, derogue el artículo R. 10-13 del CPCE, por cuanto no limitan debidamente las finalidades de la obligación de conservación generalizada e indiferenciada de los datos de tráfico y de localización. [14]

41. El Conseil d'État (Consejo de Estado) ha aludido al ajuste de las normas nacionales aquí controvertidas con la Directiva 2002/58. A su parecer, de la respuesta ofrecida por el Tribunal de Justicia en la sentencia La Quadrature du Net se infiere que debían bien inaplicarse (*écarter*) en el proceso principal (así, el artículo L. 34-1 del CPCE), [15] bien derogarse (así, el artículo R. 10-13 del CPCE). [16]

[11] *Loc. ult. cit.*

[12] Apartados 29 y 44 de los respectivos autos de reenvío.

[13] Sentencia n.º 393099 (ECLI:FR:CEASS:2021:393099.20210421). Como es lógico, en el marco de este asunto no puedo pronunciarme sobre el contenido de esa sentencia en lo que atañe a la adecuación al derecho de la Unión de alguno de sus pasajes o pronunciamientos (en particular, los relativos al acceso, con otras finalidades, a datos conservados en razón de la seguridad nacional) o a la interpretación que lleva a cabo de la sentencia La Quadrature du Net. En la vista, la Comisión declaró que estaba evaluando si procedía algún tipo de reacción contra esa sentencia, sin haber adoptado aún ninguna decisión al respecto.

[14] A instancia del Tribunal de Justicia, las partes han tenido ocasión de pronunciarse sobre esta sentencia en el curso de la vista.

[15] Apartado 58 de la sentencia del Conseil d'État (Consejo de Estado).

[16] Artículo 2 de la parte dispositiva de la sentencia del Conseil d'État (Consejo de Estado).

42. La relevancia de la sentencia La Quadrature du Net para responder a la primera pregunta prejudicial de estos reenvíos es tanto más acusada cuanto que en aquella sentencia ya se tuvo en cuenta, entre otros preceptos, el artículo R. 10-13 del CPCE,[17] que, junto con el artículo L. 34-I del mismo CPCE, son la clave para aplicar el artículo L. 621-10 del CMF.

43. Recordaré que, para recabar los datos relativos a la utilización de las líneas telefónicas empleadas por los sospechosos de las infracciones sobre las que versaba la investigación sobre un posible abuso de mercado, los agentes de la autoridad administrativa se basaron, justamente, en el artículo L. 621-10 del CMF.

3. ¿Pérdida de objeto de las peticiones de decisión prejudicial?

44. Como ya he avanzado, el tribunal de reenvío quiere saber si la normativa nacional controvertida es compatible con la Directiva 2003/6 y con el Reglamento n.º 596/2014, en la medida en que una y otro puedan ofrecer un fundamento específico para la obligación de conservación de los datos, distinto del contenido en la Directiva 2002/58.

45. Si esto es así, estimo que las peticiones de decisión prejudicial no han perdido su objeto, pese a la incidencia que sobre aquella normativa nacional pudieran tener las sentencias de los órganos jurisdiccionales franceses antes reseñadas:

— Por un lado, no cabe descartar que, según el derecho interno, el artículo R. 10-13 del CPCE pudiera desplegar algún efecto en los procedimientos principales, lo que corresponde determinar al tribunal de reenvío.

— Por otro lado, el mandato dirigido al Gobierno por el Conseil d'État (Consejo de Estado), además de comportar la obligación de derogar formalmente aquel precepto, conlleva también una serie de directrices en cuanto a las condiciones que debe reunir la normativa que se dicte en sustitución de la que ha de derogarse.[18]

46. En efecto, el Conseil d'État (Consejo de Estado) no se ha circunscrito a imponer al Gobierno la obligación de derogar el artículo R. 10-13 del CPCE en el plazo de seis meses, sino que explícitamente le conmina a «limitar las finalidades perseguidas por estos artículos y a adaptar el marco reglamentario relativo a la conservación de los datos de conexión».[19]

[17] Sentencia La Quadrature du Net, apartado 70: «Por lo que se refiere al artículo R. 10-13 del CPCE y a la obligación de conservación generalizada e indiferenciada de los datos relativos a las comunicaciones que este establece, el órgano jurisdiccional remitente […] observa que dicha conservación permite a la autoridad judicial acceder a los datos de las comunicaciones efectuadas por una persona antes de que haya sido identificada como sospechosa de haber cometido un delito, por lo que presenta una utilidad operativa sin parangón para la investigación, descubrimiento y persecución de delitos.»

[18] En la vista, el Gobierno francés informó de la aprobación de la Loi nº 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement (Ley n.º 2021/998, de 31 de julio de 2021, sobre la prevención de actos de terrorismo y los servicios de información) (JORF n.º 176, de 31 de julio de 2021). Su artículo 17 modifica el artículo L. 34-1 del CPCE. Un ulterior decreto debe determinar, «según la actividad de los operadores y la naturaleza de las comunicaciones, las informaciones y las categorías de datos conservados en aplicación de los [apartados] II *bis* y III», modificados, del artículo L. 34 del CPCE.

[19] Apartado 59 de la sentencia del Conseil d'État (Consejo de Estado). En especial, y según se desprende del artículo 1 de la parte dispositiva de dicha sentencia, la adaptación exigida deberá recoger «un reexamen periódico de la existencia de una amenaza grave, real y actual o previsible para la seguridad nacional».

47. En consecuencia, el pronunciamiento del Tribunal de Justicia en cuanto al fondo podrá ser de utilidad al tribunal de reenvío, ya que:

— La conservación de los datos de tráfico pudiera, en hipótesis, tener en la Directiva 2003/6 y en el Reglamento n.º 596/2014 un fundamento autónomo y distinto del ofrecido por la Directiva 2002/58.

— De la Directiva 2003/6 y del Reglamento n.º 596/2014 podrían resultar condiciones particulares y específicas, en lo que hace a los propósitos de la conservación de datos.

B. Primera pregunta prejudicial

48. La primera pregunta prejudicial atañe al artículo 12, apartado 2, letras a) y d), de la Directiva 2003/6 y al artículo 23, apartado 2, letras g) y h), del Reglamento n.º 596/2014.

49. Esos preceptos consienten que las autoridades administrativas competentes soliciten a las empresas de comunicaciones electrónicas (y, en su caso, a las empresas de servicios de inversión, entidades de crédito o entidades financieras), los registros [20] existentes sobre tráfico de datos y sobre datos telefónicos, cuando haya una sospecha razonable de que se ha cometido una infracción de abuso de mercado y esos registros puedan resultar relevantes para su investigación.

50. La premisa de la que parte el tribunal de reenvío es que el acceso a esos registros presupone que «el legislador nacional obliga 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 […] obtenga de la empresa de telecomunicaciones los registros existentes sobre datos de tráfico […] permitiendo, en particular, realizar un seguimiento de los contactos establecidos por los interesados antes de que surgieran las sospechas».

51. Pues bien, sobre la obligación de conservar de manera generalizada e indiferenciada los datos de conexión en ámbitos distintos de la seguridad nacional (por lo que aquí importa, en el ámbito de la lucha contra el abuso de mercado) tiene plena vigencia la jurisprudencia del Tribunal de Justicia, *recapitulada* en la sentencia La Quadrature du Net.

1. ¿Base jurídica autónoma para la obligación de conservar datos en la Directiva 2003/6 y en el Reglamento n.º 596/2014?

52. Ciertamente, la doctrina de la sentencia La Quadrature du Net se ha fijado en relación con la Directiva 2002/58, mientras que las normas traídas ahora a colación por la Cour de cassation (Tribunal de Casación) son la Directiva 2093/6 y el Reglamento n.º 596/2014.

53. Sin embargo, la Directiva 2002/58 constituye la disposición de referencia en cuanto atañe, como indica su título, al «tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas».

[20] A tenor del artículo 3 del Reglamento n.º 596/2004, se entiende por «registros de datos de tráfico» los definidos en el artículo 2, párrafo segundo, letra b), de la Directiva 2002/58, esto es, «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».

54. Tanto la Directiva 2003/6 (cuyo objeto propio son las operaciones con información privilegiada y la manipulación del mercado) como el Reglamento n.º 596/2014 (consagrado al abuso de mercado) incluyen preceptos que, como los enunciados en la primera pregunta de los presentes reenvíos, conciernen al *tratamiento* de los registros de tráfico de datos.

55. Son, por tanto, normas que, a ese específico respecto, puramente instrumental de su finalidad y de su objeto, deben interpretarse en el marco del régimen instaurado por la Directiva 2002/58.

56. Así se desprende, en mi opinión, de los artículos 12, apartado 2, letra d), de la Directiva 2003/6 y 23, apartado 2, letras g) y h), del Reglamento n.º 596/2014:

— El primero de esos preceptos versa sobre el derecho a «solicitar registros *existentes* sobre tráfico de datos»; [21]

— la letra g) del apartado 2 del artículo 23 del Reglamento n.º 596/2014 incumbe a «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»; [22]

— por último, la letra h) de ese mismo artículo 23 habla también de «los registros *existentes* sobre tráfico de datos que *mantenga* una empresa de telecomunicaciones […]». [23]

57. A mi juicio, ninguno de estos preceptos otorga habilitaciones específicas —distintas de las contempladas en la Directiva 2002/58— para *conservar* datos. Se circunscriben a autorizar a las administraciones competentes el *acceso* a los datos conservados (*existentes*) con arreglo a la normativa que disciplina, de manera general, el tratamiento de esos datos personales en el sector de las comunicaciones electrónicas, es decir, la Directiva 2002/58.

58. Tampoco el artículo 28 del Reglamento n.º 596/2014 (cuya interpretación, por lo demás, no demanda el tribunal de reenvío) podría esgrimirse como una supuesta base jurídica autónoma para imponer la obligación de conservación de datos en este ámbito.

59. Ese artículo, bajo la rúbrica «Protección de datos» y, una vez más, en cuanto al «tratamiento de datos de carácter personal»:

— Corrobora el derecho, y a la vez el deber, de las autoridades competentes, de ejercer «las funciones con las que den cumplimiento al presente Reglamento de conformidad con las disposiciones legislativas, reglamentarias o administrativas nacionales de transposición de la Directiva 95/46/CE».

21 Cursiva añadida.

22 Cursiva añadida.

23 Cursiva añadida.

— No alude a la obligación de conservar los datos [24] requerida a las empresas de comunicaciones electrónicas, limitándose a hacer una remisión a la Directiva 95/46 [25] en lo que atañe a la protección de estos.

60. El silencio de la Directiva 2003/6 y del Reglamento n.º 596/2014 en materia de la conservación de datos impuesta a los operadores de comunicaciones electrónicas es comprensible, a la vista de su cercanía temporal con la Directiva 2002/58. El legislador europeo contaba ya con esta última como marco exhaustivo de referencia para perfilar los contornos (y las excepciones) de aquella obligación, lo que hacía innecesario un régimen propio de conservación para combatir los abusos de mercado.

61. De ahí que la interpretación hecha por el Tribunal de Justicia de la Directiva 2002/58 haya de extenderse, con naturalidad, a la conservación de datos que, estando en poder de los operadores de comunicaciones electrónicas, pueden utilizar las autoridades de investigación en el marco de la lucha contra los abusos de mercado.

62. Los «registros existentes» a los que aluden la Directiva 2003/6 y el Reglamento n.º 596/2014 solo pueden ser los «registros *lícitamente* existentes», es decir, los realizados de conformidad con la Directiva 2002/58. Es esta Directiva la que, en el derecho de la Unión «establece, en particular, la armonización de las disposiciones nacionales necesarias para garantizar un nivel equivalente de protección de las libertades y los derechos fundamentales y, en particular, del derecho a la intimidad y la confidencialidad, en lo que respecta al tratamiento de los datos personales en el sector de las comunicaciones electrónicas». [26]

63. La *licitud* de los «registros existentes» solo puede justificarse cuando, en definitiva, su existencia esté amparada por lo que prescribe la Directiva 2002/58.

64. El Gobierno francés se opone a este planteamiento. Alega que la respuesta del Tribunal de Justicia debe ceñirse a la interpretación de la Directiva 2003/6 y del Reglamento n.º 596/2014. Una y otro autorizarían a los Estados miembros, de manera implícita, a implantar una obligación de conservación generalizada e indiferenciada. En otro caso, quedaría gravemente perjudicado su efecto útil.

65. No comparto los alegatos del Gobierno francés, pero, incluso de acogerlos, lo cierto es que esa pretendida «habilitación implícita» no dejaría de estar sujeta a las condiciones a las que, de acuerdo con la jurisprudencia del Tribunal de Justicia, están sometidos los Estados miembros cuando utilizan la posibilidad de imponer la obligación de una conservación generalizada e indiferenciada de datos con arreglo a la Directiva 2002/58.

[24] Sí fija, sin embargo, un período de cinco años para su conservación.

[25] Directiva derogada por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46 (Reglamento general de protección de datos) (DO 2016, L 119, p. 1). He de recordar que, en la sentencia La Quadrature du Net, apartado 210, el Tribunal de Justicia declaró que «[…] al igual que ocurre con el artículo 15, apartado 1, de la Directiva 2002/58, la facultad que el artículo 23, apartado 1, del Reglamento 2016/679 confiere a los Estados miembros solo puede ejercerse respetando la exigencia de proporcionalidad, según la cual las excepciones a la protección de los datos personales y las restricciones a dicha protección deben establecerse sin sobrepasar los límites de lo estrictamente necesario (véase, por analogía, por lo que se refiere a la Directiva 95/46, la sentencia de 7 de noviembre de 2013, IPI, C-473/12, EU:C:2013:715, apartado 39 y jurisprudencia citada)».

[26] Sentencia La Quadrature du Net, apartado 91.

66. En otras palabras, de aceptar, en hipótesis, que la Directiva 2003/6 y el Reglamento n.º 596/2014 arbitrasen un fundamento autónomo para la conservación de los datos (*quod non*), esa conservación estaría sometida a las mismas condiciones que habrían de disciplinarla si su apoyo se encontrara en cualquier otra disposición normativa de la Unión.

67. Así es porque, en última instancia, esas condiciones derivan de la salvaguarda de los derechos fundamentales garantizados por la Carta, a cuyo respeto remiten la Directiva 2003/6 y el Reglamento n.º 596/2014. Son esos derechos, justamente, los que ha esgrimido el Tribunal de Justicia en la jurisprudencia de La Quadrature du Net.

68. El propio Gobierno francés y cuantos han intervenido en este procedimiento no han podido evitar referirse a la doctrina recogida en esta última sentencia. En unos casos (como el Gobierno portugués o la Comisión), resaltando que brinda la pauta para responder a estas preguntas prejudiciales; en otros (como, en particular, el Gobierno irlandés), solicitando explícitamente su revisión.

69. El debate ocasionado por este procedimiento se ha centrado, pues, en si se ha de corroborar o revisar la doctrina del Tribunal de Justicia en relación con la licitud de la conservación generalizada e indiferenciada de datos de tráfico y de localización en el ámbito de las comunicaciones electrónicas.

2. Proscripción de la conservación generalizada e indiferenciada de datos de tráfico y medidas legislativas para proteger la seguridad nacional o para luchar contra la delincuencia grave

70. Como he defendido en las conclusiones Commissioner of the Garda Síochána y SpaceNet y Telekom Deutschland, de esta misma fecha, no creo pertinente la revisión de la jurisprudencia del Tribunal de Justicia en relación con el artículo 15, apartado 1, de la Directiva 2002/58.

71. En este contexto, los elementos indispensables para responder al tribunal de reenvío se desprenden, a mi juicio, directamente de la jurisprudencia del Tribunal de Justicia que ha *recapitulado* la sentencia La Quadrature du Net.

72. He de recordar, pues, ante todo, la doctrina del Tribunal de Justicia en esa sentencia, cuyo apartado 168 la sintetiza así:

«El artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta, debe interpretarse en el sentido de que se opone a medidas legislativas que establezcan, para los fines previstos en dicho artículo 15, apartado 1, con carácter preventivo, una conservación generalizada e indiferenciada de los datos de tráfico y de localización. En cambio, dicho artículo 15, apartado 1, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta, no se opone a medidas legislativas:

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

las condiciones y de las garantías que deben establecerse, y teniendo en cuenta que dicho requerimiento únicamente podrá expedirse por un período temporalmente limitado a lo estrictamente necesario, pero que podrá renovarse en caso de que persista dicha amenaza;

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

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

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

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

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

73. La idea medular de la jurisprudencia del Tribunal de Justicia en relación con la Directiva 2002/58 es que los usuarios de los medios de comunicación electrónicos tienen derecho a contar con que, en principio, sus comunicaciones y los datos relativos a ellas permanezcan anónimos y no puedan registrarse, salvo que medie su consentimiento. [27]

74. El artículo 15, apartado 1, de la Directiva 2002/58 admite excepciones a la obligación de garantizar la confidencialidad. La sentencia La Quadrature du Net se extiende en el examen de la conciliación de esas excepciones con los derechos fundamentales cuyo ejercicio puede verse afectado. [28]

75. La conservación generalizada e indiscriminada de los datos de trafico únicamente podría justificarse, de acuerdo con el Tribunal de Justicia, en el objetivo de la protección de la seguridad nacional, cuya importancia «supera la de los demás objetivos contemplados en el artículo 15, apartado 1, de la Directiva 2002/58». [29]

[27] Sentencia La Quadrature du Net, apartado 109.

[28] Ibidem, apartados 111 a 133.

[29] *Ibidem*, apartado 136.

76. En ese caso (seguridad nacional), el Tribunal de Justicia ha declarado que ese precepto, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta, «no se opone, en principio, a *una medida legislativa que autoriza a las autoridades competentes a instar* a los proveedores de servicios de comunicaciones electrónicas a proceder a *la conservación* de los datos de tráfico y de los datos de localización del conjunto de los usuarios de los medios de comunicaciones electrónicas *durante un período limitado*, siempre que existan circunstancias suficientemente concretas que permitan considerar que el Estado miembro en cuestión se enfrenta a una amenaza grave […] para la seguridad nacional que resulte real y actual o previsible». [30]

77. En especial, el Tribunal de Justicia entiende que el «objetivo de la protección de la seguridad nacional» «incluye la prevención y la represión de actividades que puedan desestabilizar gravemente las estructuras constitucionales, políticas, económicas o sociales fundamentales de un país, y, en particular, amenazar directamente a la sociedad, a la población o al propio Estado». [31]

78. Ahora bien, no se respetaría el sentido de la sentencia La Quadrature du Net si sus declaraciones respecto de la seguridad nacional pudieran extrapolarse a los delitos, incluso graves, que no atenten contra aquella, sino contra la seguridad pública u otros intereses jurídicamente protegidos.

79. De ahí que el Tribunal de Justicia haya distinguido cuidadosamente entre las medidas legislativas nacionales que establecen la conservación preventiva, generalizada e indiferenciada, de los datos de tráfico y de localización para proteger la seguridad nacional (apartados 134 a 139 de la sentencia La Quadrature du Net) de las que atañen a la lucha contra la delincuencia y a la protección de la seguridad pública (apartados 140 a 151 de la misma sentencia). Unas y otras no pueden tener el mismo alcance, so pena de privar a esa distinción de cualquier sentido.

80. Los instrumentos de conservación de datos de tráfico y de localización para la lucha contra la delincuencia grave se exponen, repito, en los apartados 140 a 151 de la sentencia La Quadrature du Net. A ellos hay que añadir, para la misma finalidad, los que autorizan la conservación preventiva de las direcciones IP y de los datos relativos a la identidad civil de la persona (apartados 152 a 159 de aquella sentencia), así como la «conservación rápida» de los datos de tráfico y de localización (apartados 160 a 166 de la mencionada sentencia).

81. Sin duda, los abusos de mercado son del todo reprobables, pues dañan «la integridad de los mercados financieros y la confianza del público en los valores y los instrumentos derivados». En esa misma medida, pueden calificarse, según los casos, de infracciones punibles, y en los supuestos más señalados, de delitos graves. [32]

[30] *Ibidem*, apartado 137 (cursiva añadida). Así es, continúa el Tribunal de Justicia, «aun cuando dicha medida se refiera, de modo indiscriminado, a todos los usuarios de medios de comunicaciones electrónicas sin que estos parezcan, a primera vista, guardar relación […] con una amenaza para la seguridad nacional de dicho Estado miembro», procediendo entonces «considerar que la existencia de dicha amenaza puede, por sí sola, establecer esa relación» (*loc. ult. cit.*).

[31] Sentencia La Quadrature du Net, apartado 135. Ciertamente, como destaco en el punto 39 de las conclusiones SpaceNet y Telekom Deutschland, de estas prescripciones resulta un régimen más riguroso y estricto que el que se desprende de la jurisprudencia del Tribunal Europeo de Derechos Humanos (TEDH) en relación con el artículo 8 del Convenio Europeo de los Derechos Humanos y de las Libertades Fundamentales. Así lo admite, claro está, el artículo 52, apartado 3, *in fine*, de la Carta. Sin perjuicio de que, como indico en el punto 40 de esas conclusiones, la doctrina del TEDH en sus sentencias de 25 de mayo de 2021, Big Brother Watch y otros c. Reino Unido (CE:ECHR:2021:0525JUD005817013) y Centrum för Rättvisa c. Suecia (CE:ECHR:2021:0525JUD003525208), así como en la de 4 de diciembre de 2015, Zakharov c. Rusia (CE:ECHR:2015:1204JUD004714306), conciernen a supuestos que no son equiparables a los debatidos en estos reenvíos prejudiciales. En definitiva, la solución debe encontrarse aplicando normativas nacionales que se reputen conformes con la regulación *exhaustiva* de la Directiva 2002/58, tal como la interpreta el Tribunal de Justicia.

[32] Véase la Directiva 2014/57/UE del Parlamento Europeo y del Consejo, de 16 de abril de 2014, sobre las sanciones penales aplicables al abuso de mercado (Directiva sobre abuso de mercado) (DO 2014, L 173, p. 179).

82. Por eso, al aludir a la cooperación mutua entre las autoridades competentes de los Estados miembros en la prevención y la lucha contra la delincuencia grave que afecte a dos o más Estados miembros o a un interés común protegido por una política de la Unión, el anexo I del Reglamento (UE) 2016/794 [33] engloba en aquel concepto, junto con otros conductas reprimibles, las «operaciones con información privilegiada y manipulación del mercado».

83. Ahora bien, su carácter delictivo, incluso grave cuando concurra, es el mismo que pudieran tener otras muchas infracciones que afectan a intereses públicos relevantes y a políticas de la Unión. El anexo I del Reglamento 2016/794 enumera, entre otros ejemplos de delincuencia grave, el tráfico de estupefacientes; las actividades de blanqueo de capitales; el tráfico de inmigrantes; la trata de seres humanos; los secuestros, retenciones ilegales y toma de rehenes; los delitos contra los intereses financieros de la Unión; la violación de los derechos de propiedad industrial y falsificación de mercancías; los delitos informáticos, la corrupción y los delitos contra el medio ambiente, comprendida la contaminación procedente de buques.

84. Los intereses públicos protegidos con la tipificación penal de algunas de aquellas conductas pueden tener tanta o mayor relevancia que los que se defienden al reprimir los abusos de mercado. Pero eso no significa que tales comportamientos impliquen una amenaza a la seguridad nacional, en el sentido de la sentencia La Quadrature du Net. [34]

85. Como sostuvo la Comisión en la vista, los objetivos de la Directiva 2003/6 y del Reglamento n.º 596/2014 tienden a la consecución de un mercado interior (en particular, en el sector de los mercados financieros), pero no a preservar la seguridad nacional. [35]

86. Extender la noción de «amenaza contra la seguridad nacional» a los delitos de abuso de mercado abriría la puerta a hacer lo mismo con otras muchas infracciones de intereses públicos no menos importantes, pero que difícilmente un tribunal penal encajaría en aquel concepto, mucho más restrictivo. Si el Tribunal de Justicia accediese a abrir esa puerta, el cuidadoso equilibrio que subyace en la sentencia La Quadrature du Net habría sido inútil.

87. En definitiva, los registros/grabaciones «existentes» a los que se refieren el artículo 12, apartado 2, letra d), de la Directiva 2003/6 y el artículo 23, apartado 2, letras g) y h), del Reglamento n.º 596/2914 no pueden ser sino los que la Directiva 2002/58, según la interpretación del Tribunal de Justicia, permite que se conserven para luchar contra la delincuencia grave y proteger la seguridad pública. En ningún caso pueden equiparase a los conservados de manera preventiva, generalizada e indiferenciada, para defender la seguridad nacional.

C. Segunda pregunta prejudicial

88. Con la segunda pregunta prejudicial el tribunal de reenvío quiere saber si, en el supuesto de que la normativa francesa relativa a la conservación de los datos de conexión no fuese compatible con el derecho de la Unión, pueden mantenerse provisionalmente sus efectos.

[33] Reglamento del Parlamento Europeo y del Consejo, de 11 de mayo de 2016, relativo a la Agencia de la Unión Europea para la Cooperación Policial (Europol) y por el que se sustituyen y derogan las Decisiones 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI y 2009/968/JAI del Consejo (DO 2016, L 135, p. 53).

[34] En cuanto a la posibilidad de establecer un *tertium genus* de delitos, a caballo entre la seguridad nacional y la delincuencia grave, me remito a los puntos 51 y 52 de mis conclusiones Commissioner of the Garda Síochána.

[35] Desde una posición más crítica, la defensa de VD recordó en su intervención oral cómo la seguridad nacional se ha vinculado a numerosas categorías delictivas en los sistemas políticos totalitarios, que hallan por doquier amenazas a la seguridad del Estado.

89. Dada la fecha de sus reenvíos, el tribunal *a quo* no pudo tomar en cuenta que la respuesta a sus dudas se encuentra en la sentencia (de 6 de octubre de 2020) La Quadrature du Net (en especial, en sus apartados 213 a 228), que, en este aspecto, se ha atenido a la jurisprudencia tradicional.

90. De acuerdo con el Tribunal de Justicia, apreciada una 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, «el órgano jurisdiccional remitente no puede aplicar una disposición de su derecho nacional que le faculta para limitar en el tiempo los efectos de una declaración de ilegalidad que le corresponde efectuar, con arreglo a ese derecho, con respecto a la normativa nacional controvertida en el litigio principal». [36]

91. La razón es que «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». [37] «Limitación temporal de los efectos de la interpretación de este derecho dada por el Tribunal de Justicia [que] solo puede admitirse en la propia sentencia que resuelve sobre la interpretación solicitada», [38] lo que no ha sido el caso en la sentencia 8 de abril de 2014, Digital Rights Ireland y otros. [39]

92. En consecuencia, si el Tribunal de Justicia no ha creído pertinente la limitación temporal de los efectos de su interpretación de la Directiva 2002/58, el órgano judicial remitente no puede decidir la prórroga de la eficacia de una normativa nacional incompatible con las disposiciones del derecho de la Unión que, como sucede con la Directiva 2003/6 y el Reglamento n.º 596/2014, han de interpretarse a la luz de aquella primera Directiva.

D. Tercera pregunta prejudicial

93. En la misma línea de la anterior, con su tercera pregunta prejudicial la Cour de Cassation (Tribunal de Casación) quiere saber si un órgano jurisdiccional nacional puede 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».

94. La premisa de este interrogante es, de nuevo, que esa normativa, en sí misma, resulta incompatible con el derecho de la Unión. [40] Y así lo declara el propio tribunal de reenvío: aunque la AMF sea una autoridad administrativa independiente, «la facultad atribuida a sus investigadores de obtener los datos de conexión sin control previo de un órgano jurisdiccional o de otra autoridad independiente no era conforme con las exigencias de los artículos 7, 8 y 11 de la Carta […] tal como los ha interpretado el Tribunal de Justicia». [41]

36 Sentencia La Quadrature du Net, apartado 220.

37 *Ibidem*, apartado 216.

38 *Loc. ult. cit.*

39 Asuntos C 293/12 y C 594/12 (EU:C:2014:238).

40 Como ya he recordado, el Conseil Constitutionel (Consejo Constitucional) anuló el artículo L. 621-10 del CMF. La sentencia del Conseil d'État (Consejo de Estado) de 21 de abril de 2021 reconoce, en diversos pasajes, que el acceso a los datos debe estar precedido de un control jurisdiccional o de una autoridad independiente dotada de un poder vinculante.

41 Apartados 28 y 43 de los respectivos autos de reenvío. La jurisprudencia a la que alude se remonta a la sentencia de 21 de diciembre de 2016, Tele2 Sverige y Watson y otros (C-203/15 y C-698/15, EU:C:2016:970), apartado 120.

95. A la misma solución conduce la sentencia del Tribunal de Justicia de 2 de marzo de 2021, Prokuratuur (Condiciones de acceso a los datos relativos a las comunicaciones electrónicas),[42] cuyos apartados 51 y siguientes recalcan que el acceso de las autoridades nacionales competentes a los datos conservados ha de supeditarse a un control previo, realizado bien por un órgano jurisdiccional, bien por una entidad administrativa independiente que tenga la condición de «tercero» respecto de la que solicita el acceso a esos datos.

96. En estas condiciones, la contestación a la tercera pregunta prejudicial ha de ser idéntica a la de la segunda.

V. Conclusión

97. A tenor de lo expuesto, sugiero al Tribunal de Justicia responder a la Cour de cassation (Tribunal de Casación, Francia) en los siguientes términos:

«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 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, deben interpretarse en el sentido de que se oponen a una normativa nacional que impone a las empresas de telecomunicaciones electrónicas la obligación de conservar de forma generalizada e indiferenciada los datos de tráfico en el marco de la investigación de operaciones con información privilegiada o de manipulación y abuso del mercado.

2) Un órgano jurisdiccional nacional no puede limitar en el tiempo los efectos de la incompatibilidad con el derecho de la Unión de una normativa interna que impone a los proveedores de servicios de comunicaciones electrónicas una obligación de conservación generalizada e indiferenciada de los datos de tráfico incompatible 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 relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea, y que permite a la autoridad administrativa encargada de llevar a cabo investigaciones en materia de abuso de mercado obtener la comunicación de datos de conexión sin control previo por parte de un órgano jurisdiccional o de una autoridad administrativa independiente».

[42] Asunto C-746/18, EU:C:2021:152.