Recopilación de la Jurisprudencia

CONCLUSIONES DEL ABOGADO GENERAL
M. CAMPOS SÁNCHEZ-BORDONA
presentadas el 15 de enero de 2020[1]

Asuntos acumulados C-511/18 y C-512/18

La Quadrature du Net,
French Data Network,
Fédération des fournisseurs d'accès à Internet associatifs,
Igwan.net (C-511/18)
contra
Premier ministre,
Garde des Sceaux, ministre de la Justice,
Ministre de l'Intérieur,
Ministre des Armées

[Petición de decisión prejudicial planteada por el Conseil d'État (Consejo de Estado, actuando como Tribunal Supremo de lo contencioso-administrativo, Francia)]

«Cuestión prejudicial — Tratamiento de datos de carácter personal y protección de la vida privada en el sector de las comunicaciones electrónicas — Salvaguarda de la seguridad nacional y lucha contra el terrorismo — Directiva 2002/58/CE — Ámbito de aplicación — Artículo 1, apartado 3 — Artículo 15, apartado 3 — Artículo 4 TUE, apartado 2 — Carta de los Derechos Fundamentales de la Unión Europea — Artículos 6, 7, 8, 11, 47 y 52, apartado 1 — Conservación generalizada e indiferenciada de los datos de conexión y de los datos que permitan identificar a los creadores de contenidos — Recopilación de datos de tráfico y de localización — Acceso a los datos»

1. El Tribunal de Justicia ha mantenido en los últimos años una línea jurisprudencial constante sobre la conservación y el acceso a los datos personales, de la que son hitos destacados:

– La sentencia de 8 de abril de 2014, Digital Rights Ireland y otros,[2] en la que declaró la invalidez de la Directiva 2006/24/CE[3] porque permitía una injerencia desproporcionada en los derechos reconocidos por los artículos 7 y 8 de la Carta de Derechos Fundamentales de la Unión Europea (en adelante, «la Carta»).

– La sentencia de 21 de diciembre de 2016, Tele2 Sverige y Watson y otros,[4] en la que interpretó el artículo 15, apartado 1, de la Directiva 2002/58/CE.[5]

1 Lengua original: español.

2 Asuntos C-293/12 y C-594/12, en lo sucesivo, «sentencia Digital Rights», EU:C:2014:238.

3 Directiva del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE (DO 2006, L 105, p. 54).

4 Asuntos C-203/15 y C-698/15, en lo sucesivo, «sentencia Tele2 Sverige y Watson», EU:C:2016:970.

5 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).

– La sentencia de 2 de octubre de 2018, Ministerio Fiscal,[6] en la que confirmó la interpretación de ese mismo precepto de la Directiva 2002/58.

2. Esas sentencias (en particular, la segunda) preocupan a las autoridades de algunos Estados miembros, pues, a su entender, tienen como consecuencia despojarles de un instrumento que reputan necesario para la salvaguarda de la seguridad nacional y para la lucha contra la criminalidad y el terrorismo. De ahí que algunos de esos Estados miembros aboguen por revocar o matizar aquella jurisprudencia.

3. Determinados órganos jurisdiccionales de los Estados miembros han puesto de relieve esa misma preocupación en cuatro reenvíos prejudiciales,[7] respecto de los que, con esta misma fecha se leen mis conclusiones.

4. Los cuatro asuntos suscitan, ante todo, el problema de la aplicación de la Directiva 2002/58 a actividades relacionadas con la seguridad nacional y la lucha contra el terrorismo. Si aquella Directiva rigiese en ese contexto, habrá de dilucidarse, acto seguido, en qué medida pueden los Estados miembros restringir los derechos de privacidad que protege. En último lugar, se deberá analizar hasta qué punto las diferentes normativas nacionales (la británica,[8] la belga[9] y la francesa[10]) sobre esta materia se atienen al derecho de la Unión, tal como ha sido interpretado por el Tribunal de Justicia.

I. Marco normativo

A. Derecho de la Unión

1. Directiva 2002/58

5. A tenor del 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 Comunidad.

[…]

3. La presente Directiva no se aplicará a las actividades no comprendidas en el ámbito de aplicación del Tratado constitutivo de la Comunidad Europea, 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 dichas actividades estén relacionadas con la seguridad del mismo) y a las actividades del Estado en materia penal.»

6 Asunto C-207/16, en lo sucesivo, «sentencia Ministerio Fiscal», EU:C:2018:788.

7 Además de estos dos (asuntos C-511/18 y C-512/18), los asuntos C-623/17, Privacy International, y C-520/18, Ordre des barreaux francophones et germanophone y otros.

8 Asunto Privacy International, C-623/17.

9 Asunto Ordre des barreaux francophones et germanophone y otros, C-520/18.

10 Asuntos La Quadrature du Net y otros, C-511/18 y C-512/18

6. El artículo 3 («Servicios afectados») señala:

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

7. El apartado 1 del artículo 5 («Confidencialidad de las comunicaciones») recoge:

«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».

8. El artículo 6 («Datos de tráfico») preceptúa:

«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».

9. El artículo 15 («Aplicación de determinadas disposiciones de la Directiva 95/46/CE [11]»), apartado 1, indica:

«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».

11 Directiva 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).

2. Directiva 2000/31/CE[12]

10. El artículo 14 prescribe:

«1. Los Estados miembros garantizarán que, cuando se preste un servicio de la sociedad de la información consistente en almacenar datos facilitados por el destinatario del servicio, el prestador de servicios no pueda ser considerado responsable de los datos almacenados a petición del destinatario, a condición de que:

[…]

3. El presente artículo no afectará la posibilidad de que un tribunal o una autoridad administrativa, de conformidad con los sistemas jurídicos de los Estados miembros, exijan al prestador de servicios de poner fin a una infracción o impedirla, ni a la posibilidad de que los Estados miembros establezcan procedimientos por los que se rija la retirada de datos o impida el acceso a ellos».

11. Según el artículo 15:

«1. Los Estados miembros no impondrán a los prestadores de servicios una obligación general de supervisar los datos que transmitan o almacenen, ni una obligación general de realizar búsquedas activas de hechos o circunstancias que indiquen actividades ilícitas, respecto de los servicios contemplados en los artículos 12, 13 y 14.

2. Los Estados miembros podrán establecer obligaciones tendentes a que los prestadores de servicios de la sociedad de la información comuniquen con prontitud a las autoridades públicas competentes los presuntos datos ilícitos o las actividades ilícitas llevadas a cabo por destinatarios de su servicio o la obligación de comunicar a las autoridades competentes, a solicitud de estas, información que les permita identificar a los destinatarios de su servicio con los que hayan celebrado acuerdos de almacenamiento».

3. Reglamento (UE) 2016/679[13]

12. Con arreglo al artículo 2 («Ámbito de aplicación material»):

«1. El presente Reglamento se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.

2. El presente Reglamento no se aplica al tratamiento de datos personales:

a) en el ejercicio de una actividad no comprendida en el ámbito de aplicación del derecho de la Unión;

b) por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del TUE;

c) efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas;

12 Directiva del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico) (DO 2000, L 178, p. 1).

13 Reglamento 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).

d) por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención.

[…]»

13. A tenor del apartado 1 del artículo 23 («Limitaciones»):

«El derecho de la Unión o de los Estados miembros que se aplique al responsable o el encargado del tratamiento podrá limitar, a través de medidas legislativas, el alcance de las obligaciones y de los derechos establecidos en los artículos 12 a 22 y el artículo 34, así como en el artículo 5 en la medida en que sus disposiciones se correspondan con los derechos y obligaciones contemplados en los artículos 12 a 22, cuando tal limitación respete en lo esencial los derechos y libertades fundamentales y sea una medida necesaria y proporcionada en una sociedad democrática para salvaguardar:

a) la seguridad del Estado;

b) la defensa;

c) la seguridad pública;

d) la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención;

e) otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un interés económico o financiero importante de la Unión o de un Estado miembro, inclusive en los ámbitos fiscal, presupuestario y monetario, la sanidad pública y la seguridad social;

f) la protección de la independencia judicial y de los procedimientos judiciales;

g) la prevención, la investigación, la detección y el enjuiciamiento de infracciones de normas deontológicas en las profesiones reguladas;

h) una función de supervisión, inspección o reglamentación vinculada, incluso ocasionalmente, con el ejercicio de la autoridad pública en los casos contemplados en las letras a) a e) y g);

i) la protección del interesado o de los derechos y libertades de otros;

j) la ejecución de demandas civiles.»

14. El artículo 95 («Relación con la Directiva 2002/58/CE») reza:

«El presente Reglamento no impondrá obligaciones adicionales a las personas físicas o jurídicas en materia de tratamiento en el marco de la prestación de servicios públicos de comunicaciones electrónicas en redes públicas de comunicación de la Unión en ámbitos en los que estén sujetas a obligaciones específicas con el mismo objetivo establecidas en la Directiva 2002/58/CE.»

B. Derecho nacional

1. Code de la sécurité intérieure (Código de seguridad interior)

15. De acuerdo con el artículo L. 851-1:

«En las condiciones establecidas en el capítulo 1 del título II del presente libro, podrá autorizarse recopilar de los operadores de comunicaciones electrónicas y de las personas mencionadas en el artículo L. 34-1 del code des postes et des communications électroniques [(Código de correos y comunicaciones electrónicas)], así como de las personas indicadas en el artículo 6, punto I, apartados 1 y 2, de la loi n.º 2004-575 […] pour la confiance dans l'économie numérique [(Ley n.º 2004-575 […], para la confianza en la economía digital)], información o documentos tratados o conservados por sus redes o servicios de comunicaciones electrónicas, incluidos los datos técnicos relativos a la identificación de los números de abonado o de conexión a servicios de comunicaciones electrónicas, a la relación de todos los números de abonado o de conexión de una persona determinada, a la localización de los equipos terminales utilizados y a las comunicaciones de un abonado correspondientes a la relación de números de llamadas entrantes y salientes, la duración y la fecha de las comunicaciones [...]».

16. En los artículos L. 851-2 y L. 851-4 se regula, en función de las distintas finalidades y modalidades, el acceso administrativo en tiempo real a los datos de conexión conservados de este modo.

17. El artículo L. 851-2 autoriza, exclusivamente con fines de prevención del terrorismo, a recopilar, de esas mismas personas, la información o los documentos que menciona el artículo L. 851-1. Esta recopilación, referida solo a una o a varias personas previamente identificadas como sospechosas de estar relacionadas con una amenaza terrorista, se efectúa en tiempo real. Lo mismo sucede con el artículo L. 851-4, que autoriza la transmisión en tiempo real por los operadores únicamente de los datos técnicos relativos a la localización de los equipos terminales. [14]

18. El artículo L. 851-3 permite imponer a los operadores de comunicaciones electrónicas y a los prestadores de servicios técnicos la obligación de «aplicar en sus redes tratamientos automatizados de datos destinados, en función de los parámetros establecidos en la autorización, a detectar conexiones que pudieran suponer una amenaza terrorista». [15]

19. El artículo L. 851-5 especifica que, en determinadas condiciones, «puede autorizarse la utilización de un dispositivo técnico que permita la localización en tiempo real de una persona, de un vehículo o de un objeto».

20. De conformidad con el apartado I del artículo L. 851-6, es posible, en ciertas condiciones, «recoger […] directamente, por medio de un aparato o de un dispositivo técnico mencionado en el apartado 1 del artículo 226-3 del code pénal [(Código penal)], los datos técnicos de conexión que permitan la identificación de un equipo terminal o del número de abonado de su usuario, así como los datos relativos a la localización de los equipos terminales utilizados».

14 Según el órgano jurisdiccional de remisión, estas técnicas no crean para los prestadores de servicios una obligación de conservación suplementaria a la que se requiere para la facturación y comercialización de sus servicios, así como para la prestación de servicios de valor añadido.

15 Según el órgano jurisdiccional de remisión, esta técnica, que no implica una conservación generalizada e indiferenciada, únicamente persigue recopilar, durante un tiempo limitado, de entre todos los datos de conexión tratados por esas personas, los que pudieran estar relacionados con una infracción grave de ese tipo.

2. Código de correos y comunicaciones electrónicas

21. A tenor del artículo L. 34-1, en su versión aplicable a los hechos:

«I. El presente artículo se aplicará al tratamiento de datos personales en 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 consiste en ofrecer acceso a servicios de comunicación al público en línea, eliminarán o anonimizarán todos los datos de tráfico, sin perjuicio de lo estipulado 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 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 du code de la défense [(Código de defensa)], podrán aplazarse durante un periodo máximo de un año las operaciones dirigidas a eliminar o a anonimizar determinadas categorías de datos técnicos. Mediante decreto consultado al Conseil d'État [(Consejo de Estado)], adoptado tras el dictamen de la Commission nationale de l'informatique et des libertés [(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 fijadas en los apartados III, IV y V versarán exclusivamente sobre la identificación de los usuarios de los servicios suministrados por los operadores, 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 a las informaciones consultadas, bajo cualquier forma, en el marco de esas comunicaciones.

La conservación y el tratamiento de los datos se realizará en el respeto de las disposiciones de la 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 estos datos para otros fines distintos de los previstos en el presente artículo».

22. En virtud del artículo R. 10-13, apartado I, los operadores deben conservar, a los fines de la investigación, de la constatación y de la persecución de las infracciones penales, los siguientes datos:

«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».

23. De acuerdo con el apartado II del mismo precepto, en el caso de las actividades de telefonía el operador debe conservar, además, los datos que faciliten identificar el origen y la localización de la comunicación.

24. Con arreglo al apartado III del mismo artículo, los datos mencionados deben conservarse durante un año, desde el día de su registro.

3. 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 para la confianza en la economía digital)

25. El párrafo primero del apartado II del artículo 6 de la Ley 2004-575 establece que las personas cuya actividad consiste en ofrecer acceso a servicios de comunicación al público en línea y 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, «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».

26. El párrafo tercero del apartado II del mismo precepto señala que la autoridad judicial podrá requerir a estas personas que comuniquen los datos mencionados en el párrafo primero.

27. Según el último párrafo del apartado II, mediante decreto del Conseil d'État (Consejo de Estado) «se definirán los datos mencionados en el párrafo primero y se determinarán la duración y las modalidades de su conservación». [16]

16 La definición se llevó a cabo mediante el décret n.º 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne (Decreto n.º 2011-219, de 25 de febrero de 2011, sobre la conservación de los datos que permitan la identificación de toda persona que haya contribuido a la creación de un contenido ofrecido en línea). De ese Decreto pueden destacarse: a) El artículo 1, apartado 1, a cuyo tenor quienes brindan acceso a servicios de comunicación en línea deben conservar los siguientes datos: el identificador de la conexión, el identificador atribuido al abonado, el identificador de la terminal utilizada para la conexión, la fecha y hora del inicio y el fin de la conexión, las características de la línea del abonado; b) En virtud del apartado 2 del artículo 1, quienes 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 deben conservar, para cada operación, los datos siguientes: el identificador de la conexión en el origen de la comunicación, el identificador atribuido al contenido objeto de la operación, los tipos de protocolos utilizados para la conexión al servicio y para la transferencia de contenidos, la naturaleza de la operación, la fecha y la hora de la operación, el identificador utilizado por el autor de la operación; y c) En fin, el apartado 3 del artículo 1 preceptúa que las personas mencionadas en los dos apartados precedentes deben conservar las siguientes informaciones facilitadas por un utilizador al suscribir un contrato o crear una cuenta: el identificador de la conexión al crear la cuenta; nombre, apellidos o razón social; las direcciones postales asociadas, los pseudónimos utilizados, las direcciones de correo electrónico o de cuenta asociadas, los números de teléfono, la palabra clave puesta al día y los datos que permitan verificarla o modificarla.

II. Hechos y cuestiones prejudiciales planteadas

A. Asunto C-511/18

28. La Quadrature du Net, French Data Network, Igwan.net y la Fédération des fournisseurs d'accès à internet associatifs (en lo sucesivo, «recurrentes») demandaron ante el Conseil d'État (Consejo de Estado) la anulación de varios decretos de desarrollo de algunas disposiciones del Código de seguridad interior. [17]

29. Los recurrentes sostenían, en síntesis, que tanto los decretos impugnados como esas disposiciones del Código de seguridad interior eran contrarios a los derechos al respeto de la vida privada, a la protección de datos personales y a un recurso efectivo, garantizados respectivamente por los artículos 7, 8 y 47 de la Carta.

30. En tal tesitura, el Conseil d'État (Consejo de Estado) plantea al Tribunal de Justicia las siguientes preguntas:

«1) ¿Debe considerarse la obligación de conservación generalizada e indiferenciada, impuesta a los prestadores de servicios al amparo de las disposiciones habilitantes del artículo 15, apartado 1, de la Directiva 2002/58 […], en un contexto caracterizado por amenazas graves y persistentes para la seguridad nacional, en particular por el riesgo terrorista, una injerencia justificada por el derecho a la seguridad reconocido en el artículo 6 de la Carta […] y las exigencias de la seguridad nacional, cuya responsabilidad incumbe únicamente a los Estados miembros en virtud del artículo 4 [TUE]?

2) ¿Debe interpretarse la Directiva 2002/58 […], a la luz de la Carta […], en el sentido de que permite medidas legislativas, tales como las medidas de recopilación en tiempo real de datos de tráfico y localización de personas concretas, que, si bien afectan a los derechos y obligaciones de los proveedores de servicios de comunicaciones electrónicas, no les imponen sin embargo una obligación específica de conservación de sus datos?

3) ¿Debe interpretarse la Directiva 2002/58 […], a la luz de la Carta […], en el sentido de que supedita en todos los casos la legalidad de los procedimientos de recopilación de los datos de conexión a la obligación de informar a las personas afectadas, cuando tal información ya no pueda poner en peligro las investigaciones efectuadas por las autoridades competentes, o cabe considerar que dichos procedimientos son legales habida cuenta de todas las demás garantías de procedimiento existentes, siempre que estas últimas aseguren la efectividad del derecho a recurrir?»

17 Los decretos impugnados eran los siguientes: a) décret n.º 2015-1885 du 28 septembre 2015 portant désignation des services spécialisés de renseignement (Decreto n.º 2015-1185, de 28 de septiembre de 2015, de designación de servicios especializados de información); b) décret n.º 2015-1211 du 1er octubre 2015 relatif au contentieux de la mise en oeuvre des techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'État (Decreto n.º 2015-1211, de 1 de octubre de 2015, relativo a los recursos sobre la aplicación de técnicas de información sujetas a autorización y ficheros que afecten a la seguridad del Estado); c) décret n.º 2015-1639 du 11 décembre 2015 relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du libre VIII du code de la sécurité intérieure (Decreto n.º 2015-1639, de 11 de diciembre de 2015, relativo a la designación de servicios, distintos de los servicios especializados de información, autorizados a utilizar las técnicas mencionadas en el título V del libro VIII del Código de seguridad interior); y d) décret n.º 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement (Decreto n.º 2016-67, de 29 de enero de 2016, relativo a las técnicas de recopilación de información).

B. Asunto C-512/18

31. Los recurrentes en el litigio que ha dado lugar al asunto C-511/18, con excepción de Igwan.net, interesaron también del Conseil d'État (Consejo de Estado) que anulara la desestimación (por silencio administrativo) de su solicitud de derogación del artículo R. 10-13 del code des postes et des communications électroniques (Código de correos y comunicaciones electrónicas) y del Decreto n.º 2011-219 de 25 de febrero de 2011.

32. A juicio de esos recurrentes, las normas impugnadas imponen una obligación de conservación de datos de tráfico, de localización y de conexión que, por su carácter general, constituye un atentado desproporcionado a los derechos al respeto de la vida privada y familiar, a la protección de datos de carácter personal y a la libertad de expresión, protegidos por los artículos 7, 8 y 11 de la Carta, con infracción del artículo 15, apartado 1, de la Directiva 2002/58.

33. En ese recurso, el Conseil d'État (Consejo de Estado) ha formulado esta cuestión prejudicial:

«1) ¿Debe considerarse la obligación de conservación generalizada e indiferenciada, impuesta a los proveedores de servicios sobre la base de las disposiciones habilitantes del artículo 15, apartado 1, de la Directiva 2002/58 […], en particular a la vista de las garantías y de los controles que acompañan posteriormente la recogida y la utilización de estos datos de conexión, una injerencia justificada por el derecho a la seguridad garantizado en el artículo 6 de la Carta […] y las exigencias de la seguridad nacional, cuya responsabilidad incumbe únicamente a los Estados miembros en virtud del artículo 4 [TUE]?

2) ¿Deben interpretarse las disposiciones de la Directiva 2000/31, a la luz de los artículos 6, 7, 8 y 11, así como 52, apartado 1, de la Carta […], en el sentido de que permiten a un Estado miembro establecer una normativa nacional que obligue a las personas cuya actividad consista en ofrecer acceso a servicios de comunicación al público en línea y a 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, a conservar los datos que puedan permitir la identificación de quien haya contribuido a la creación del contenido o de alguno de los contenidos de los servicios que aquellas prestan, con el fin de que la autoridad judicial pueda requerir, en su caso, la comunicación de los mismos para que se respeten las normas en materia de responsabilidad civil o penal?»

III. Procedimiento ante el Tribunal de Justicia y posiciones de las partes

34. Las cuestiones prejudiciales se registraron en el Tribunal de Justicia el 3 de agosto de 2018.

35. Han depositado observaciones escritas La Quadrature du Net, la Fédération des fournisseurs d'accès à Internet associatifs, French Data Network, los Gobiernos alemán, belga, británico, checo, chipriota, danés, español, estonio, francés, húngaro, irlandés, polaco y sueco, además de la Comisión.

36. El 9 de septiembre de 2019 tuvo lugar una vista pública, celebrada conjuntamente con las de los asuntos C-623/17, Privacy International, y C-520/18, Ordre des barreaux francophones et germanophone y otros, en la que comparecieron las partes de los cuatro reenvíos prejudiciales, los Gobiernos antes citados y los de los Países Bajos y Noruega, así como la Comisión y el Supervisor europeo para la protección de datos personales.

IV. Análisis

37. Las preguntas del Conseil d'État (Consejo de Estado) pueden agruparse en tres:

– En primer lugar, si es compatible con el derecho de la Unión una normativa nacional que impone a los proveedores de servicios de comunicaciones electrónicas la obligación de conservar de manera generalizada e indiferenciada los datos de conexión (primera pregunta en el asunto C-511/18 y en el asunto C-512/18) y, en particular, los datos que permitan identificar a los creadores de los contenidos ofrecidos por dichos proveedores (segunda pregunta en el asunto C-512/18).

– En segundo lugar, si la licitud de los procedimientos de recopilación de datos de conexión está condicionada, en todo caso, a la obligación de informar a las personas afectadas, cuando no se pongan en peligro las investigaciones (tercera pregunta en el asunto C-511/18).

– En tercer lugar, si la recopilación en tiempo real de datos de tráfico y de localización, sin obligación de conservarlos, es compatible —y en qué condiciones— con la Directiva 2002/58 (segunda pregunta en el asunto C-511/18).

38. Se trata de determinar, en definitiva, si es acorde con el derecho de la Unión una normativa nacional que impone a los proveedores de servicios de comunicaciones electrónicas dos tipos de obligaciones: a) por un lado, la *recopilación* de ciertos datos, pero no su conservación; b) por otro lado, la *conservación* de los datos de conexión y de los que facilitan la identificación de los creadores de los contenidos de los servicios prestados por tales proveedores.

39. Con carácter previo habrá de dirimirse si, justamente en razón del contexto [18] en el que esa normativa nacional se ha promulgado (esto es, en circunstancias en las que puede verse comprometida la seguridad nacional) resulta aplicable la Directiva 2002/58.

A. Sobre la aplicabilidad de la Directiva 2002/58

40. El órgano judicial de remisión da por sentado que la normativa objeto de litigio se enmarca en el ámbito de aplicación de la Directiva 2002/58. Así se desprende, a su juicio, de la doctrina fijada en la sentencia Tele2 Sverige y Watson y corroborada en la sentencia Ministerio Fiscal.

41. Por el contrario, algunos de los Gobiernos que han intervenido en el procedimiento afirman que la normativa controvertida no está comprendida en dicho ámbito. Para defender su postura, traen a colación, entre otros argumentos, la sentencia de 30 de mayo de 2006, Parlamento/Consejo y Comisión. [19]

42. Coincido con el Conseil d'État (Consejo de Estado) en que la sentencia Tele2 Sverige y Watson ha zanjado esta parte del debate, confirmando que la Directiva 2002/58 se aplica, en principio, cuando los proveedores de servicios electrónicos se ven obligados por la ley a conservar los datos de sus abonados y a permitir a las autoridades públicas que accedan a ellos. No cambia esa tesis que las obligaciones se impongan a los proveedores por razones de seguridad nacional.

43. Debo avanzar, ya desde este momento, que, si hubiera alguna discordancia entre la sentencia Tele2 Sverige y Watson y las precedentes, debería tenerse como prevalente aquella, en cuanto posterior y revalidada por la sentencia Ministerio Fiscal. Creo, sin embargo, que no existe esa discordancia, según trataré de explicar.

18 «Un contexto […] [de] amenazas graves y persistentes para la seguridad nacional, en particular por el riesgo terrorista», según se especifica en la primera pregunta del asunto C-511/18.

19 Asuntos C-317/04 y C-318/04, en lo sucesivo «sentencia Parlamento/Consejo y Comisión», EU:C:2006:346.

1. Sentencia Parlamento/Consejo y Comisión

44. Los asuntos zanjados por la sentencia Parlamento/Consejo y Comisión versaban sobre:

– El Acuerdo entre la Comunidad Europea y los Estados Unidos de América relativo al tratamiento y a la transferencia de los datos PNR [Passenger Name Records (datos de los expedientes de los pasajeros)] por las compañías aéreas a las autoridades estadounidenses. [20]

– El carácter adecuado de la protección de los datos personales contenidos en los registros de nombres de los pasajeros, transferidos a dichas autoridades. [21]

45. El Tribunal de Justicia concluyó que la transferencia de esos datos era un tratamiento que tenía por objeto la seguridad pública y las actividades del Estado en materia penal. Con arreglo al artículo 3, apartado 2, primer guion, de la Directiva 95/46, las dos Decisiones controvertidas no se hallaban en el ámbito de aplicación de la Directiva 95/46.

46. Los datos eran inicialmente recopilados por las compañías aéreas en el marco de una actividad —la venta de billetes— perteneciente a la esfera de aplicación del derecho de la Unión. Sin embargo, su tratamiento, tal como se contemplaba en la Decisión controvertida, «no es necesario para la realización de una prestación de servicios, sino que se considera necesario para salvaguardar la seguridad pública y para fines represivos». [22]

47. El Tribunal de Justicia adoptó así un enfoque teleológico, atendiendo al propósito buscado con el tratamiento de los datos: de perseguirse con él la protección de la seguridad pública, debía reputarse extramuros del ámbito de aplicación de la Directiva 95/46. Ahora bien, ese propósito no era el único criterio determinante, [23] por lo que la sentencia subrayó que «se inserta en un marco creado por los poderes públicos y cuyo objetivo es proteger la seguridad pública». [24]

20 Decisión 2004/496/CE del Consejo, de 17 de mayo de 2004, relativa a la celebración de un Acuerdo entre la Comunidad Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de los datos de los expedientes de los pasajeros por las compañías aéreas al Departamento de seguridad nacional, Oficina de aduanas y protección de fronteras, de los Estados Unidos (DO 2004, L 183, p. 83, y corrección de errores en DO 2005, L 255, p. 168) (asunto C-317/04).

21 Decisión 2004/535/CE de la Comisión, de 14 de mayo de 2004, relativa al carácter adecuado de la protección de los datos personales incluidos en los registros de nombres de los pasajeros que se transfieren al Servicio de aduanas y protección de fronteras de los Estados Unidos (DO 2004, L 235, p. 11) (asunto C-318/04).

22 Sentencia Parlamento/Consejo y Comisión, apartado 57. En el apartado 58 se insiste en que el «hecho de que los datos […] sean recogidos por operadores privados con fines mercantiles y de que sean estos quienes organizan su transferencia a un Estado tercero» no implica que esa transferencia no constituya uno de los supuestos de inaplicación de la Directiva 95/46 enumerados en el artículo 3, apartado 2, primer guion, de esta última, pues «esta transferencia se inserta en un marco creado por los poderes públicos y cuyo objetivo es proteger la seguridad pública».

23 Así lo destacaría, ulteriormente, el añorado abogado general Bot en sus conclusiones del asunto Irlanda/Parlamento y Consejo (C-301/06, EU:C:2008:558). Afirmaba que la sentencia Parlamento/Consejo y Comisión «no puede significar […] que solo el examen de la finalidad pretendida por un tratamiento de datos de carácter personal sea pertinente para incluir o, en su caso, excluir, ese tratamiento del ámbito de aplicación del sistema de protección de datos establecido por la Directiva 95/46. Es preciso también verificar en el marco de qué tipo de actividades se realiza un tratamiento de datos. Únicamente en el caso de que dicho tratamiento se haya puesto en práctica para el ejercicio de actividades propias del Estado o de las autoridades estatales y ajenas a la esfera de actividades de los particulares estará excluido del sistema comunitario de protección de datos de carácter personal establecido por la Directiva 95/46, y ello con arreglo al artículo 3, apartado 2, primer guion, de esa Directiva» (punto 122).

24 Sentencia Parlamento/Consejo y Comisión, apartado 58. El Acuerdo tenía por objeto principal exigir a las compañías aéreas con servicios de transporte de pasajeros entre la Unión y los Estados Unidos que facilitaran a las autoridades norteamericanas un acceso electrónico a los datos PNR de los expedientes de nombres de pasajeros obrantes en sus sistemas informáticos de control de reservas y de salidas. Instauraba, pues, una forma de cooperación internacional entre la Unión y los Estados Unidos para luchar contra el terrorismo y otros crímenes graves, intentando conciliar ese objetivo con el de la protección de los datos personales de los pasajeros. En ese contexto, la obligación impuesta a las compañías no era muy distinta de un intercambio directo de datos entre autoridades públicas.

48. La sentencia Parlamento/Consejo y Comisión permite, pues, apreciar la diferencia entre la cláusula de exclusión y las cláusulas de restricción o limitación de la Directiva 95/46 (análogas a las de la Directiva 2002/58). Es verdad, sin embargo, que unas y otras se refieren a objetivos de interés general similares, lo que genera alguna confusión respecto de su alcance respectivo, como advertía en su momento el abogado general Bot. [25]

49. Es probable que esta confusión se encuentre en el origen de la tesis defendida por los Estados miembros que abogan por la inaplicabilidad de la Directiva 2002/58 a este contexto. A su juicio, el interés de la seguridad nacional solo se salvaguarda mediante la exclusión recogida en el artículo 1, apartado 3, de la Directiva 2002/58. Lo cierto es, sin embargo, que también sirven a ese mismo interés las limitaciones autorizadas por el artículo 15, apartado 1, de la reiterada Directiva, entre ellas, la relativa a la seguridad nacional. Este último precepto sería superfluo si la Directiva 2002/58 resultase inaplicable ante cualquier invocación de la seguridad nacional.

2. Sentencia Tele2 Sverige y Watson

50. En la sentencia Tele2 Sverige y Watson se afrontó si eran compatibles con el derecho de la Unión algunos regímenes nacionales que imponían a los proveedores de servicios de comunicación electrónica accesibles para el público una obligación general de conservar los datos relativos a dichas comunicaciones. Los supuestos eran, por tanto, sustancialmente idénticos a los que se dirimen en estos reenvíos prejudiciales.

51. Planteada de nuevo la aplicabilidad del derecho de la Unión —ahora ya bajo la cobertura de la Directiva 2002/58—, el Tribunal de Justicia comenzó señalando que «el alcance del ámbito de aplicación de la Directiva 2002/58 debe apreciarse teniendo en cuenta en especial la sistemática de esta última». [26]

52. En esa perspectiva, el Tribunal de Justicia advirtió que, «[c]iertamente, las medidas legales contempladas en el artículo 15, apartado 1, de la Directiva 2002/58 se refieren a actividades propias de los Estados o de las autoridades estatales, ajenas a los ámbitos de actividad de los particulares […] Además, las finalidades a las que deben responder tales medidas en virtud de dicha disposición, en el presente caso la salvaguarda de la seguridad nacional […], coinciden en esencia con las finalidades que persiguen las actividades mencionadas en el artículo 1, apartado 3, de dicha Directiva». [27]

53. Así pues, la finalidad de las medidas que, con arreglo al artículo 15, apartado 1, de la Directiva 2002/58, pueden adoptar los Estados miembros para limitar el derecho a la privacidad coincide (en este punto) con la que justifica eximir a ciertas actividades estatales del régimen de la Directiva, conforme a su artículo 1, apartado 3.

54. Sin embargo, el Tribunal de Justicia entendió que, «a la vista de la sistemática de la Directiva 2002/58», aquella circunstancia no permitía «llegar a la conclusión de que las medidas legales contempladas en el artículo 15, apartado 1, de la Directiva 2002/58 están excluidas del ámbito de aplicación de dicha Directiva, ya que esto privaría de toda eficacia a dicha disposición. En efecto, esta disposición presupone necesariamente que las medidas nacionales que se mencionan en ella […] están comprendidas en el ámbito de aplicación de esa misma Directiva, dado que esta solo autoriza expresamente a los Estados miembros a adoptarlas cumpliendo los requisitos que establece». [28]

25 Conclusiones del abogado general Bot en el asunto Irlanda/Parlamento y Consejo (C-301/06, EU:C:2008:558), punto 127.

26 Sentencia Tele2 Sverige y Watson, apartado 67.

27 *Ibidem*, apartado 72.

28 *Ibidem*, apartado 73.

55. A lo anterior se añade que las limitaciones autorizadas por el artículo 15, apartado 1, de la Directiva 2002/58 «regulan, a los efectos mencionados en dicha disposición, la actividad de los proveedores de servicios de comunicaciones electrónicas». De ahí que ese precepto, puesto en relación con el artículo 3 de la Directiva, «debe interpretarse en el sentido de que tales medidas legales están comprendidas en el ámbito de aplicación de la misma Directiva».[29]

56. En consecuencia, el Tribunal de Justicia sostuvo que se incluyen en el ámbito de aplicación de la Directiva 2002/58 tanto una medida legal que imponga a los proveedores «la obligación de conservar los datos de tráfico y de localización, puesto que dicha actividad implica necesariamente el tratamiento, por ellos, de datos personales»,[30] como la que regule el acceso de las autoridades a los datos conservados por esos proveedores.[31]

57. La interpretación de la Directiva 2002/58 asumida por el Tribunal de Justicia en la sentencia Tele2 Sverige y Watson se reitera en la sentencia Ministerio Fiscal.

58. ¿Podría afirmarse que la sentencia Tele2 Sverige y Watson representa un giro, más o menos implícito, respecto de la doctrina sentada en la sentencia Parlamento/Consejo y Comisión? Así lo entiende, por ejemplo, el Gobierno de Irlanda, para quien solo esta última sería compatible con la base jurídica de la Directiva 2002/58 y respetuosa con el artículo 4 TUE, apartado 2.[32]

59. El Gobierno francés, por su parte, estima que podría salvarse la contradicción si se repara en que la doctrina de la sentencia Tele2 Sverige y Watson alude a actividades de los Estados miembros en el ámbito del derecho penal, mientras que la establecida en la sentencia Parlamento/Consejo y Comisión tiene que ver con la seguridad del Estado y la defensa. Así, la doctrina de la sentencia Tele2 Sverige y Watson no sería aplicable al supuesto ahora analizado, en el que habría de estarse a la solución adoptada en la sentencia Parlamento/Consejo y Comisión.[33]

60. Como ya he avanzado, creo que puede encontrase una vía de integración entre ambas sentencias, distinta de la auspiciada por el Gobierno francés. No comparto esta última, pues, en mi opinión las consideraciones de la sentencia Tele2 Sverige y Watson referidas explícitamente a la lucha contra el terrorismo[34] son extensibles a cualquier otra amenaza contra la seguridad nacional (de las que el terrorismo es una más).

3. Posibilidad de una interpretación integradora de la sentencia Parlamento/Consejo y Comisión con la sentencia Tele2 Sverige y Watson

61. A mi juicio, en las sentencias Tele2 Sverige y Watson y Ministerio Fiscal el Tribunal de Justicia tuvo en cuenta la razón de ser de las cláusulas de exclusión y de restricción, así como la relación sistemática entre los dos tipos de cláusulas.

62. Si en el asunto Parlamento/Consejo y Comisión el Tribunal de Justicia afirmó que el tratamiento de los datos era ajeno al ámbito de la Directiva 95/46, se debió, como ya he recordado, a que, en el contexto de la cooperación entre la Unión Europea y los Estados Unidos, en un marco típicamente internacional, debía prevalecer la dimensión estatal de la actividad frente al hecho de que aquel tratamiento comportara también una dimensión mercantil o privada. Una de las cuestiones debatidas entonces era, justamente, la base jurídica apropiada para la Decisión controvertida.

29 *Ibidem*, apartado 74.

30 *Ibidem*, apartado 75.

31 *Ibidem*, apartado 76.

32 Apartados 15 y 16 de las observaciones escritas del Gobierno irlandés.

33 Apartados 34 a 50 de las observaciones escritas del Gobierno francés.

34 Sentencia Tele2 Sverige y Watson, apartados 103 y 119.

63. Por el contrario, respecto de las medidas nacionales examinadas en las sentencias Tele2 Sverige y Watson y Ministerio Fiscal, el Tribunal de Justicia colocó en primer plano el alcance interno del tratamiento de datos: el marco normativo en el que este se realizaba era exclusivamente nacional, careciendo, por tanto, de la dimensión exterior que caracterizaba el objeto de la sentencia Parlamento/Consejo y Comisión.

64. El diferente peso de las dimensiones internacional e interna (mercantil y privada) del tratamiento de datos tuvo como consecuencia que, en el primer caso, se impusiera la cláusula de exclusión del derecho de la Unión como más adecuada para la protección del interés general cifrado en la seguridad nacional. En el segundo, por el contrario, ese mismo interés podía ser eficazmente atendido mediante la cláusula de limitación prevista en el artículo 15, apartado 1, de la Directiva 2002/58.

65. Aún cabría apreciar otra divergencia, ligada al diferente contexto normativo: cada una de esas sentencias se centró en la interpretación de dos preceptos que, más allá de su apariencia, no son iguales.

66. Así, la sentencia Parlamento/Consejo y Comisión se pronunció sobre la interpretación del artículo 3, apartado 2, de la Directiva 95/46, mientras que la sentencia Tele2 Sverige y Watson se hizo sobre el artículo 1, apartado 3, de la Directiva 2002/58. La lectura atenta de esos artículos pone de manifiesto una disparidad suficiente para respaldar el sentido de los pronunciamientos del Tribunal de Justicia en uno y en otro caso.

67. Con arreglo al artículo 3, apartado 2, de la Directiva 95/46, «[l]as disposiciones de la presente Directiva *no se aplicarán al tratamiento de datos personales* […] efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del derecho comunitario […] y, en cualquier caso, *al tratamiento de datos* que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dicho *tratamiento* esté relacionado con la seguridad del Estado) y las actividades del Estado en materia penal».[35]

68. Por su parte, conforme al artículo 1, apartado 3 de la Directiva 2002/58, esta última «*no se aplicará a las actividades* no comprendidas en el ámbito de aplicación del Tratado constitutivo de la Comunidad 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 dichas *actividades* estén relacionadas con la seguridad del mismo) y a las actividades del Estado en materia penal».[36]

69. Mientras el artículo 3, apartado 2, de la Directiva 95/46 excluye el *tratamiento de datos* que tenga por objeto —en lo que aquí interesa— la seguridad del Estado, el artículo 1, apartado 3, de la Directiva 2002/58 lo hace con las *actividades* dirigidas a preservar —también en lo que aquí importa— la seguridad estatal.

70. La diferencia no es baladí. La Directiva 95/46 dejaba fuera de su ámbito de aplicación una actividad (el «tratamiento de datos personales») que cualquiera puede realizar. De esa actividad quedaban específicamente exceptuados los tratamientos cuyo objeto fuera, entre otros, la seguridad del Estado. Era irrelevante, en cambio, la naturaleza del *sujeto* que llevara a cabo el tratamiento de los datos. El enfoque adoptado para la identificación de las acciones excluidas era, pues, teleológico o finalista, y sin distinción de personas en cuanto a sus actores.

35 Cursiva añadida.

36 Cursiva añadida.

71. Se entiende así que, en el asunto Parlamento/Consejo y Comisión, el Tribunal de Justicia atendiera primordialmente a la finalidad perseguida con el tratamiento de datos. No importaba el «hecho de que los datos […] sean recogidos por operadores privados con fines mercantiles y de que sean estos quienes organizan su transferencia a un Estado tercero», pues lo fundamental era que «esta transferencia se inserta en un marco creado por los poderes públicos y cuyo objetivo es proteger la seguridad pública». [37]

72. En cambio, «las actividades que tienen por objeto la seguridad del Estado», ajenas al ámbito de aplicación de la Directiva 2002/58 analizado en el asunto Tele2 Sverige y Watson, no pueden predicarse de cualquier sujeto, sino únicamente del Estado mismo. Además, no se integran en ellas las funciones normativas o reguladoras del Estado, sino estrictamente las actuaciones materiales de los poderes públicos.

73. En efecto, las *actividades* enumeradas en el artículo 1, apartado 3, de la Directiva 2002/58 «son, en todos los casos, actividades propias del Estado o de las autoridades estatales y ajenas a la esfera de actividades de los particulares». [38] Ahora bien, esas «actividades» no pueden ser de naturaleza normativa. Si así fuera, todas las disposiciones adoptadas por los Estados miembros en relación con el tratamiento de datos personales quedarían fuera del ámbito de la Directiva 2002/58, a poco que pretendieran justificarse como necesarias para garantizar la seguridad del Estado.

74. Por un lado, esto supondría una notable pérdida para la eficacia de dicha Directiva, pues la mera invocación de un concepto jurídico tan indeterminado como el de la seguridad nacional bastaría para hacer inaplicables frente a los Estados miembros las salvaguardas ideadas por el legislador de la Unión para proteger los datos personales de los ciudadanos. Esa protección es impracticable sin el concurso de los Estados miembros y su garantía se asegura, para el ciudadano, también frente a los poderes públicos nacionales.

75. Por otro lado, una interpretación del concepto «actividades estatales» que comprendiera las que se traducen en la promulgación de normas y disposiciones jurídicas privaría de sentido al artículo 15 de la Directiva 2002/58, que justamente habilita a los Estados miembros para —por razones de protección, *inter alia*, de la seguridad nacional— adoptar «medidas legales» con el propósito de recortar el alcance de ciertos derechos y obligaciones recogidos en la misma Directiva. [39]

76. Como destacó el Tribunal de Justicia en el asunto Tele2 Sverige y Watson, «el alcance del ámbito de aplicación de la Directiva 2002/58 debe apreciarse teniendo en cuenta en especial la sistemática de esta última». [40] Desde esa perspectiva, la interpretación del artículo 1, apartado 3, y del artículo 15, apartado 1, de la Directiva 2002/58 que los dota de sentido sin pérdida de su eficacia es la que identifica, en el primero de ambos preceptos, una exclusión material referida a las *actividades* desempeñadas por los Estados miembros en el ámbito de la seguridad nacional (y equivalentes) y, en el segundo, una habilitación para dictar *medidas legales* (esto es, normas con fuerza general) que, en aras de la seguridad nacional, afecten a las actividades de los individuos sujetos al *imperium* de los Estados miembros, restringiendo los derechos garantizados por la Directiva 2002/58.

37 Parlamento/Consejo y Comisión, apartado 58.

38 Sentencia Ministerio Fiscal, apartado 32. En el mismo sentido, sentencia Tele2 Sverige y Watson, apartado 72.

39 Sería difícil sostener, en efecto, que el artículo 15, apartado 1, de la Directiva 2002/58 permite limitar los derechos y obligaciones establecidos que proclama en un ámbito que, como el de la seguridad nacional, estaría, por principio fuera de su ámbito de aplicación, en virtud del artículo 1, apartado 3, de la propia Directiva. Como afirmó el Tribunal de Justicia en la sentencia Tele2 Sverige y Watson, apartado 73, el artículo 15, apartado 1, de la Directiva 2002/58 «presupone necesariamente que las medidas nacionales que se mencionan en ella […] están comprendidas en el ámbito de aplicación de esa misma Directiva, dado que esta solo autoriza expresamente a los Estados miembros a adoptarlas cumpliendo los requisitos que establece».

40 Sentencia Tele2 Sverige y Watson, apartado 67.

4. Exclusión de la seguridad nacional en la Directiva 2002/58

77. La seguridad nacional (o su expresión sinónima, «la seguridad del Estado», como destaca su artículo 15, apartado 1) es objeto de una doble consideración en la Directiva 2002/58. Por un lado, constituye una causa de *exclusión* (de la aplicación de esa Directiva) para todas aquellas actividades de los Estados miembros que, específicamente, la «tengan por objeto». Por otro lado, se presenta como una causa de *limitación*, que ha de desarrollarse por ley, de los derechos y las obligaciones establecidos en la Directiva 2002/58, es decir, respecto de actividades de naturaleza privada o mercantil y ajenas al dominio de las actividades regalianas. [41]

78. ¿A qué actividades se refiere el artículo 1, apartado 3, de la Directiva 2002/58? A mi juicio, el propio Conseil d'État (Consejo de Estado) ofrece un buen ejemplo al mencionar los artículos L. 851-5 y L. 851-6 del Código de seguridad interior, aludiendo a las «técnicas de recopilación de información que son aplicadas directamente por el Estado, pero no regulan las actividades de los proveedores de servicios de comunicaciones electrónicas imponiéndoles obligaciones específicas». [42]

79. Creo que ahí reside la clave para discernir el ámbito de exclusión del artículo 1, apartado 3, de la Directiva 2002/58. No estarán sujetas a su régimen las *actividades* que, dirigidas a preservar la seguridad nacional, realicen por su cuenta los poderes públicos, sin requerir la colaboración de particulares y, por tanto, sin imponerles obligaciones en su gestión empresarial.

80. El elenco de actividades de los poderes públicos excepcionadas del régimen general del tratamiento de los datos personales ha de ser, sin embargo, interpretado restrictivamente. En concreto, no puede extenderse la noción de *seguridad nacional*, cuya responsabilidad corresponde con carácter exclusivo a cada Estado miembro según el artículo 4 TUE, apartado 2, a otros sectores, más o menos próximos, de la vida pública.

81. Como en estas cuestiones prejudiciales concurre la implicación de particulares (es decir, de quienes prestan a los usuarios los servicios de comunicaciones electrónicas) y no la mera intervención de las autoridades estatales, no será necesario abundar en la delimitación de los contornos de la seguridad nacional *stricto sensu*.

82. Estimo, sin embargo, que puede valer de orientación el criterio de la Decisión marco 2006/960/JAI, [43] cuyo artículo 2, letra a), distingue entre los servicios de seguridad en sentido amplio —que comprenden «la autoridad nacional policial, aduanera u otra, autorizada según el derecho interno a descubrir, prevenir e investigar delitos y actividades delictivas y a ejercer la autoridad y adoptar medidas coercitivas en el contexto de esas actividades»—, por un lado, y las «agencias o unidades que traten especialmente cuestiones de seguridad nacional», por otro lado. [44]

41 Como señalaba, de manera incidental, el abogado general Saugmandsgaard Øe en sus conclusiones en el asunto Ministerio Fiscal (C-207/16, EU:C:2018:300), punto 47, «es preciso no confundir, por un lado, los datos personales tratados *directamente* en el marco de actividades —de índole regaliana— del Estado en un ámbito incluido en el derecho penal, y por otro, las tratadas en el marco de actividades —de naturaleza mercantil— de un prestador de servicios de comunicaciones electrónicas que *después* emplean las autoridades estatales competentes».

42 Apartados 18 y 21 del auto de reenvío en el asunto C-511/18.

43 Decisión marco del Consejo, de 18 de diciembre de 2016, sobre la simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la Unión Europea (DO 2006, L 386, p. 89).

44 En esa misma línea, el artículo 1, apartado 4, de la Decisión marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal (DO 2008, L 350, p. 60), preveía que «no afectará a los intereses esenciales de seguridad del Estado ni a las actividades específicas de inteligencia en el sector de la seguridad del Estado».

83. En el considerando décimo primero de la Directiva 2002/58 se afirma que esta, «al igual que la Directiva 95/46 […], no aborda la protección de los derechos y las libertades fundamentales en relación con las actividades no regidas por el derecho [de la Unión]». Así pues, la Directiva 2002/58 «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 del Estado […]».

84. Hay, en efecto, una continuidad entre la Directiva 95/46 y la Directiva 2002/58 en lo que hace a las competencias de los Estados miembros sobre la seguridad nacional. Ninguna de las dos tiene por objeto la protección de los derechos fundamentales en ese específico campo, en el que las actividades de los Estados miembros no están «regidas por el derecho [de la Unión]».

85. El «equilibrio» al que se refiere aquel considerando resulta de la necesidad de respetar las competencias de los Estados miembros en materia de seguridad nacional, cuando las ejercen *de manera directa y por sus propios medios*. Por el contrario, cuando, incluso por esas mismas razones de seguridad nacional, se requiere el concurso de particulares, a quienes se imponen ciertas obligaciones, esta circunstancia determina la entrada en un ámbito (la protección de la privacidad exigible a esos actores privados) regido por el derecho de la Unión.

86. Tanto la Directiva 95/46 como la Directiva 2002/58 procuran alcanzar ese equilibrio autorizando que los derechos de los particulares puedan verse limitados en virtud de medidas normativas adoptadas por los Estados al amparo de sus artículos 13, apartado 1, y 15, apartado 1, respectivamente. No hay en este punto ninguna diferencia entre ambas.

87. En cuanto al Reglamento n.º 2016/679, que configura un (nuevo) marco general para la protección de datos personales, su artículo 2, apartado 2, descarta que rija el «tratamiento de datos personales» cuando los Estados miembros «lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del TUE».

88. Así como en la Directiva 95/46 el tratamiento de datos personales estaba cualificado solo por su finalidad, con abstracción del sujeto que lo llevara a cabo, en el Reglamento n.º 2016/679 los tratamientos excluidos se identifican tanto por su finalidad como por sus autores: se exceptúan los realizados por los Estados miembros en el ejercicio de una *actividad* no comprendida en el ámbito de aplicación del derecho de la Unión [letras a) y b) del apartado 2 del artículo 2], y los ejecutados por las autoridades *con fines de lucha contra las infracciones penales y de protección* frente a las amenazas a la seguridad pública. [45]

89. La identificación de esas actividades del poder público ha de ser forzosamente restrictiva, so pena de privar de eficacia a la normativa de la Unión en materia de protección de la privacidad. El Reglamento n.º 2016/679 contempla en su artículo 23 —en la línea del artículo 15, apartado 1, de la Directiva 2002/58— la limitación, *mediante medidas legislativas*, de los derechos y las obligaciones que establece, cuando sea necesario para salvaguardar, entre otros objetivos, la seguridad del Estado, la defensa o la seguridad pública. Una vez más, si bastara la protección de esos objetivos para determinar la exclusión del ámbito de aplicación del Reglamento n.º 2016/679, sería superflua la invocación de la seguridad del Estado como justificante de la restricción, a través de medidas legislativas, de los derechos garantizados por aquel Reglamento.

45 El Reglamento n.º 2016/679 excluye, en efecto, el tratamiento de datos hecho por los Estados miembros en el ejercicio de una *actividad* que no se engloba en el ámbito de aplicación del derecho de la Unión, además del ejecutado por las autoridades *con fines de protección* de la seguridad pública.

90. Al igual que sucede con la Directiva 2002/58, no sería coherente que las medidas legislativas previstas en el artículo 23 del Reglamento n.º 2016/679 (que, repito, autoriza limitaciones estatales a los derechos de privacidad de los ciudadanos por razones de seguridad del Estado) entren en el ámbito aplicación de este y, a la vez, que la cobertura de la seguridad del Estado convierta en inaplicable, sin más, el propio Reglamento, lo que implicaría la ausencia de reconocimiento de derecho subjetivo alguno.

B. Confirmación y posibilidades de desarrollo de la jurisprudencia Tele2 Sverige y Watson

91. En mis conclusiones del asunto C-520/18 llevo a cabo un análisis detallado [46] de la jurisprudencia del Tribunal de Justicia en esta materia, a resultas del que propongo su confirmación, a la vez que sugiero alguna vía interpretativa para perfilar su contenido.

92. Me remito a ese análisis, que no estimo imprescindible transcribir ahora por mera economía. Las reflexiones que a continuación haré sobre las cuestiones prejudiciales suscitadas por el Conseil d'Etat (Consejo de Estado) han de leerse, pues, teniendo como presupuesto los epígrafes correspondientes de las conclusiones del asunto C-520/18.

C. Respuesta a las cuestiones prejudiciales

1. Sobre la obligación de conservación de los datos (primera pregunta prejudicial en los asuntos C-511/18 y C-512/18 y segunda pregunta prejudicial del asunto C-512/18)

93. En cuanto a la obligación de conservación de datos impuesta a los proveedores de servicios de comunicaciones electrónicas, el tribunal de reenvío quiere saber, en concreto:

– Si esa obligación, exigible al amparo del artículo 15, apartado 1, de la Directiva 2002/58, constituye una injerencia justificada por el «derecho a la seguridad» que garantiza el artículo 6 de la Carta y por imperativos de seguridad nacional (pregunta primera en los asuntos C-511/18 y C-512/18, así como pregunta tercera del asunto C-511/18).

– Si la Directiva 2000/31 consiente la conservación de datos que puedan permitir la identificación de quienes hayan contribuido a la creación de los contenidos accesibles al público en línea (segunda pregunta en el asunto C-512/18).

a) Consideración preliminar

94. El Conseil d'État (Consejo de Estado) alude a los derechos fundamentales reconocidos en los artículos 7 (respeto de la vida privada y familiar), 8 (protección de datos de carácter personal) y 11 (libertad de expresión y de información) de la Carta. Tales son, en efecto, los que, según el Tribunal de Justicia, podrían verse afectados por la obligación de conservar datos de tráfico que las autoridades nacionales imponen a los proveedores de servicios de comunicaciones electrónicas. [47]

95. El tribunal de reenvío alude también al derecho a la seguridad protegido por el artículo 6 de la Carta. Más que como derecho eventualmente afectado, lo invoca como factor que pudiera legitimar la imposición de aquella obligación.

46 Puntos 27 a 68.

47 Así, sentencia Tele2 Sverige y Watson, apartado 92, con cita, por analogía, de la sentencia Digital Rights, apartados 25 y 70.

96. Coincido con la Comisión en que la invocación del artículo 6 en esos términos puede resultar equívoca. Al igual que la Comisión, estimo que el precepto no ha de interpretarse en el sentido de que tiene aptitud «para imponer a la Unión una obligación positiva de adoptar medidas dirigidas a proteger a las personas contra actos criminales». [48]

97. La seguridad garantizada por aquel artículo de la Carta no se identifica con la seguridad pública. O, si se prefiere, tiene tanto que ver con esta última como cualquier otro derecho fundamental, en la medida en que la seguridad pública es una condición indispensable para el disfrute de los derechos y libertades fundamentales.

98. Según recuerda la Comisión, el artículo 6 de la Carta se corresponde con el artículo 5 del Convenio Europeo de Derechos Humanos (en los sucesivo, «CEDH»), como se asevera en las explicaciones que la acompañan. De la lectura del artículo 5 del CEDH se desprende que la «seguridad» que en él se protege es estrictamente la seguridad personal, entendida como garantía del derecho a la libertad física frente a la detención o el internamiento arbitrarios. La seguridad, en definitiva, de que nadie puede ser privado de su libertad, salvo en los casos, con los requisitos y de conformidad con los procedimientos establecidos por la ley.

99. Se trata, por tanto, de la *seguridad personal*, referida a las condiciones en las que puede restringirse la libertad física de las personas, [49] y no de la *seguridad pública* inherente a la existencia del Estado, que es presupuesto imprescindible, en una sociedad desarrollada, para conciliar el ejercicio de las potestades públicas con el disfrute de los derechos individuales.

100. Algunos Gobiernos, sin embargo, piden que se tenga más en cuenta el derecho a la seguridad en el segundo de esos sentidos. En realidad, el Tribunal de Justicia no lo ha ignorado, es más, lo ha mencionado expresamente en sus sentencias [50] y dictámenes. [51] Nunca ha negado la importancia de los objetivos de interés general de protección de la seguridad nacional y del orden público, [52] de lucha contra el terrorismo internacional en el mantenimiento de la paz y la seguridad internacionales y de lucha contra los delitos graves para garantizar la seguridad pública, [53] que ha calificado, acertadamente, de «primordial». [54] Como señaló en su día, «la protección de la seguridad pública también contribuye a la protección de los derechos y libertades de los demás». [55]

101. Se podría aprovechar la oportunidad que brindan estos reenvíos prejudiciales para proponer más claramente la búsqueda de un equilibrio entre el derecho a la seguridad, por una parte, y el derecho a la intimidad y el derecho a la protección de los datos personales, por otra parte. Así se evitarían las críticas de favorecer a los segundos en detrimento del primero.

48 Apartado 37 del escrito de observaciones de la Comisión.

49 Así lo interpreta el TEDH. Por todas, la sentencia de 5 de julio de 2016, Buzadji c. República de Moldavia, ECHR:2016:0705JUD002375507, en cuyo § 84 se afirma que el propósito fundamental del derecho reconocido por el artículo 5 del CEDH es prevenir la privación arbitraria o injustificada de la libertad individual.

50 Sentencia Digital Rights, apartado 42.

51 Dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017 (en lo sucesivo, «Dictamen 1/15», EU:C:2017:592), apartado 149 y jurisprudencia citada.

52 Sentencia de 15 de febrero de 2016, N. (C-601/15 PPU, EU:C:2016:84), apartado 53.

53 Sentencia Digital Rights, apartado 42 y jurisprudencia citada.

54 *Ibidem*, apartado 51.

55 Dictamen 1/15, apartado 149.

102. A ese equilibrio aluden, en mi opinión, el considerando décimo primero y el artículo 15, apartado 1, de la Directiva 2002/58, cuando hablan de los requisitos de necesidad y proporcionalidad de las medidas *en una sociedad democrática*. El derecho a la seguridad, repito, es consustancial a la propia existencia y supervivencia de una democracia, lo que justifica que se tenga plenamente en cuenta en el contexto de la valoración de aquella proporcionalidad. En otras palabras, si la preservación del principio de confidencialidad de los datos es primordial en una sociedad democrática, tampoco debe subestimarse la importancia de su seguridad.

103. El contexto de las amenazas graves y persistentes a la seguridad nacional y, en particular, el riesgo de terrorismo, debe, pues, tenerse en cuenta, en la línea de lo afirmado en la última frase del apartado 119 de la sentencia Tele2 Sverige y Watson. Un sistema nacional podrá responder de un modo proporcional a la naturaleza e intensidad de las amenazas a las que se enfrenta, sin que necesariamente esa respuesta haya de ser idéntica a la de otros Estados miembros.

104. Debo añadir, en fin, que las reflexiones anteriores no obstan a que, en situaciones propiamente *excepcionales*, caracterizadas por una amenaza inminente o por un riesgo extraordinario que justifiquen la declaración oficial de la situación de emergencia en un Estado miembro, la legislación nacional contemple, por un tiempo limitado, la posibilidad de imponer una obligación de conservación de datos tan amplia y general como se considere imprescindible. [56]

105. En consecuencia, la primera pregunta de ambos reenvíos prejudiciales debería reformularse, dirigiéndola, más bien, a la posibilidad de justificar la injerencia en motivos de seguridad nacional. La duda versaría, pues, sobre si la obligación impuesta a los operadores de servicios de comunicaciones electrónicas es compatible con el artículo 15, apartado 1, de la Directiva 2002/58.

b) Apreciación

1) Caracterización de las normas internas, tal como se exponen en los dos reenvíos prejudiciales, a la luz de la doctrina del Tribunal de Justicia

106. Ateniéndonos a los autos de remisión, la normativa controvertida en los procesos de origen obliga a conservar los datos:

– a los operadores de comunicaciones electrónicas y, en especial, a quienes ofrecen acceso a servicios de comunicación al público en línea; y

– a las personas físicas o jurídicas que almacenen, incluso a título gratuito, para la puesta a disposición del público en línea, señales, escritos, sonidos, imágenes o mensajes de cualquier naturaleza proporcionados por destinatarios de estos servicios. [57]

107. Los operadores deben conservar, durante un año a contar desde el día de su registro, las informaciones que permitan identificar al usuario, los datos relativos a los equipos terminales de comunicaciones utilizados, las características técnicas, la fecha, la hora y la duración de cada llamada, los datos relativos a los servicios complementarios solicitados o empleados y sus proveedores, así como los datos que faciliten identificar al destinatario de la comunicación y, en el caso de las actividades de telefonía, el origen y la localización de la comunicación. [58]

56 Véanse los puntos 105 a 107 de mis conclusiones en el asunto C-520/18.

57 Así resulta del artículo L. 851-1 del Código de seguridad interior, que remite al artículo L. 34-1 del Código de correos y comunicaciones electrónicas y al artículo 6 de la Ley n.º 2004-575, para la confianza de la economía digital.

58 Así lo expone el artículo R. 10-13 del Código de correos y comunicaciones electrónicas.

108. Tratándose, en especial, de los servicios de acceso a internet y de los servicios de almacenamiento, la normativa nacional parece demandar la conservación de las direcciones IP, [59] las claves de acceso y, si media la suscripción de un contrato o cuenta de pago, el tipo de pago efectuado, así como su referencia, el importe, la fecha y la hora de la transacción. [60]

109. Esta obligación de conservación se exige con vistas a la investigación, la constatación y la persecución de las infracciones penales. [61] Es decir, a diferencia —como se mostrará— de lo que sucede con la obligación de *recopilar* datos de tráfico y de localización, el deber de *conservarlos* no tiene como único objetivo la prevención del terrorismo. [62]

110. En cuanto a las condiciones de *acceso* a los datos conservados, de la información aportada a los autos se desprende que bien son las previstas para el régimen común (intervención de la autoridad judicial) o bien tal acceso se restringe a agentes individualmente designados y habilitados, previa autorización del Primer ministro emitida sobre la base del dictamen no vinculante de una autoridad administrativa independiente. [63]

111. Es fácil advertir que, como ha señalado la Comisión, [64] los datos cuya conservación requieren las normas nacionales se corresponden, sustancialmente, con los examinados por el Tribunal de Justicia en las sentencias Digital Rights y Tele2 Sverige y Watson. [65] Al igual que entonces, esos datos son objeto de una «obligación de conservación generalizada e indiferenciada», según destaca, con toda franqueza, el Conseil d'État (Consejo de Estado) al inicio de sus preguntas prejudiciales.

112. Si eso es así, lo que en definitiva ha de valorar el tribunal de reenvío, no cabe sino concluir que la normativa en cuestión comporta una «injerencia […] en los derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta [que] tiene una gran magnitud y debe considerarse especialmente grave». [66]

113. Ninguna de las partes personadas ha puesto en duda que una normativa de estas características conlleva una injerencia en aquellos derechos. No es preciso detenerse ahora en ese punto, ni siquiera para recordar que el menoscabo de esos derechos redunda inevitablemente en perjuicio de los fundamentos mismos de una sociedad que pretende respetar, entre otros valores, la privacidad personal que auspicia la Carta.

114. La aplicación de la doctrina instaurada en la sentencia Tele2 Sverige y Watson y ratificada en la sentencia Ministerio Fiscal llevaría con naturalidad a sostener que una normativa como la aquí controvertida «excede […] de 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, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta». [67]

59 Corresponde al tribunal de reenvío verificar este extremo, sobre el que se expresaron discrepancias en la vista.

60 Artículo 1 del Decreto n.º 2011-219.

61 Artículo R. 10-13 del Código de correos y comunicaciones electrónicas.

62 Tanto La Quadrature du Net como la Fédération des founisseurs d'accès à Internet associatifs subrayan la amplitud de los fines a los que sirve la conservación, la facultad de apreciación discrecional atribuida a las autoridades, la ausencia de criterios objetivos en su definición y la relevancia concedida a formas de criminalidad que no pueden calificarse de graves.

63 La Commission nationale de contrôle des techniques de renseignement (Comisión nacional de control de las técnicas de información). Véanse, al respecto, los apartados 145 a 148 del escrito de observaciones del Gobierno francés.

64 Apartado 60 del escrito de observaciones de la Comisión.

65 En realidad, van un poco más allá, pues también parecen contemplarse, en el caso de los servicios de acceso a internet, la conservación de la dirección IP o de las claves de acceso.

66 Sentencia Tele2 Sverige y Watson, apartado 100.

67 *Ibidem*, apartado 107.

115. En efecto, al igual que la analizada en la sentencia Tele2 Sverige y Watson, también la que ahora nos ocupa «cubre de manera generalizada a todos los abonados y usuarios registrados y […] tiene por objeto todos los medios de comunicación electrónica, así como todos los datos de tráfico [y] no establece ninguna diferenciación, limitación o excepción en función del objetivo que se pretende lograr».[68] En consecuencia, «se aplica incluso a las personas de las que no existe ningún indicio para pensar que su comportamiento pueda tener una relación, incluso indirecta o remota, con la comisión de delitos graves», y esto sin admitir ninguna excepción, «por lo que se aplica también a personas cuyas comunicaciones están sujetas a secreto profesional conforme al derecho nacional».[69]

116. Así también, la normativa litigiosa «no exige ninguna relación entre los datos cuya conservación se establece y una amenaza para la seguridad pública. En particular, no está limitada a una conservación de datos referentes a un período temporal, una zona geográfica o un círculo de personas que puedan estar implicadas de una manera u otra en un delito grave, ni a personas que por otros motivos podrían contribuir, mediante la conservación de sus datos, a la lucha contra la delincuencia».[70]

117. De lo que precede se infiere que esa normativa «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, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta».[71]

118. Lo anterior fue suficiente para que el Tribunal de Justicia concluyera que las correlativas normas nacionales no eran compatibles con el artículo 15, apartado 1, de la Directiva 2002/58, en la medida en que consagraban, «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».[72]

119. El interrogante que ahora surge es si la doctrina del Tribunal de Justicia en materia de conservación de datos personales puede, si no replantearse, al menos, matizarse cuando el propósito al que sirve esa conservación «generalizada e indiferenciada» es la lucha contra el terrorismo. La primera pregunta del asunto C-511/18 se formula, justamente, «en un contexto caracterizado por amenazas graves y persistentes para la seguridad nacional, en particular por el riesgo terrorista».

120. Ahora bien, siendo ese el *contexto fáctico* en el que se impone la obligación de conservación de los datos, lo cierto es que en su *contexto normativo* no se atiende únicamente al terrorismo. El régimen de conservación y acceso a los datos que se debate en el proceso ante el Conseil d'État (Consejo de Estado) supedita aquella obligación a los fines de la investigación, la constatación y la persecución de las infracciones penales con carácter general.

121. En todo caso, recordaré que la lucha contra el terrorismo no quedó al margen de las argumentaciones de la sentencia Tele2 Sverige y Watson, sin que el Tribunal de Justicia estimara entonces que esa modalidad delictiva precisara alguna inflexión en su doctrina.[73]

122. Por tanto, y en principio, entiendo que la pregunta del órgano judicial de remisión, centrada en la especificidad de la amenaza terrorista, debería responderse en el mismo sentido en el que se pronunció el Tribunal de Justicia en la sentencia Tele2 Sverige y Watson.

68 *Ibidem*, apartado 105.

69 *Loc. ult. cit.*

70 Sentencia Tele2 Sverige y Watson, apartado 106.

71 *Ibidem*, apartado 107.

72 *Ibidem*, apartado 112.

73 *Ibidem*, apartado 103.

123. Como sostuve en las conclusiones del asunto Stichting Brein, «[l]a certeza en la aplicación del derecho impone a los órganos jurisdiccionales si no la aplicación del *stare decisis* en términos absolutos, sí la prudencia de atenerse a lo que ellos mismos hayan decidido, tras madura reflexión, sobre un problema jurídico dado».[74]

2) Conservación de datos restringida, ante las amenazas contra la seguridad del Estado, incluida la terrorista.

124. ¿Sería posible, no obstante, matizar o completar esa doctrina, a la vista de sus consecuencias para la lucha contra el terrorismo o para la protección del Estado frente a otras amenazas análogas contra la seguridad nacional?

125. Ya he subrayado que la sola conservación de datos personales implica una injerencia en los derechos garantizados por los artículos 7, 8 y 11 de la Carta.[75] Al margen de que, en última instancia, lo que con ella se pretende es posibilitar el *acceso*, retrospectivo o simultáneo, a los datos en un momento determinado,[76] la mera conservación de datos que excedan de lo estrictamente indispensable para la transmisión de una comunicación o para la facturación de los servicios prestados por el proveedor supone la inobservancia de los límites previstos en los artículos 5 y 6 de la Directiva 2002/58.

126. Los usuarios de esos servicios (en realidad, la casi totalidad de los ciudadanos en las sociedades más desarrolladas) disfrutan, o deben disfrutar, de una expectativa legítima en el sentido de que, de no mediar su consentimiento, no se conservarán más datos suyos que los almacenados de acuerdo con aquellos preceptos. Las excepciones del artículo 15, apartado 1, de la Directiva 2002/58 han de leerse a partir de esta premisa.

127. Como ya he explicado, el Tribunal de Justicia rechazó en la sentencia Tele2 Sverige y Watson, también en relación con la lucha contra el terrorismo, la conservación generalizada e indiferenciada de los datos personales.[77]

128. Frente a las críticas recibidas, no creo que la doctrina sentada en esa sentencia minusvalore la amenaza terrorista, en cuanto forma de delincuencia particularmente grave que comporta un propósito explícito de contestación a la autoridad del Estado y de desestabilización o destrucción de sus instituciones. La lucha antiterrorista es, literalmente, vital para el Estado y su éxito, un objetivo de interés general irrenunciable para un Estado de derecho.

74 Asunto C-527/15, EU:C:2016:938, punto 41.

75 Tal y como ha rememorado el Tribunal de Justicia en el Dictamen 1/15, apartado 124, «la comunicación de datos de carácter personal a un tercero, como una autoridad pública, constituye una injerencia en el derecho fundamental consagrado en el artículo 7 de la Carta, cualquiera que sea la utilización posterior de la información comunicada. Lo mismo puede decirse de la conservación de los datos de carácter personal y del acceso a esos datos con vistas a su utilización por parte de las autoridades públicas. A este respecto, carece de relevancia que la información relativa a la vida privada de que se trate tenga o no carácter sensible o que los interesados hayan sufrido o no inconvenientes en razón de tal injerencia».

76 Como señalaba el abogado general Cruz Villalón en las conclusiones del asunto Digital Rights, C-293/12 y C-594/12 (EU:C:2013:845), punto 72, «la recogida y sobre todo la conservación, en bases de datos gigantescas, de los múltiples datos generados o tratados en el marco de la mayor parte de las comunicaciones electrónicas corrientes de los ciudadanos de la Unión constituyen una injerencia caracterizada en su vida privada, aun cuando no hagan más que crear las condiciones de posibilidad de un control retrospectivo de sus actividades tanto personales como profesionales. La recopilación de estos datos crea las condiciones de una vigilancia que, aunque solo se ejerce retrospectivamente en el momento de su explotación, amenaza no obstante de manera permanente, durante todo su período de conservación, el derecho de los ciudadanos de la Unión al secreto de su vida privada. El sentimiento difuso de vigilancia generado suscita de manera especialmente acusada la cuestión de la duración de conservación de los datos».

77 Sentencia Tele2 Sverige y Watson, apartado 103: «no puede […] justificar que una normativa nacional que establezca la conservación generalizada e indiferenciada de todos los datos de tráfico y de localización deba ser considerada necesaria a los efectos de dicha lucha».

129. Prácticamente todos los Gobiernos personados en el procedimiento, además de la Comisión, han coincidido en señalar que, más allá de sus dificultades técnicas, una conservación parcial y diferenciada de datos personales privaría a los servicios de inteligencia nacional de la posibilidad de acceder a informaciones indispensables para la identificación de amenazas para la seguridad pública y la defensa del Estado, así como para la persecución de los autores de atentados terroristas. [78]

130. Frente a esta apreciación me parece pertinente señalar que la lucha antiterrorista no ha de plantearse únicamente pensando en su eficacia. De ahí su dificultad, pero también su grandeza cuando sus medios y sus métodos se ajustan a las exigencias del Estado de derecho, que es, ante todo, sujeción del poder y de la fuerza a los límites del derecho y, en especial, a un orden jurídico que tiene en la defensa de los derechos fundamentales la razón y el fin de su existencia.

131. Si para el terrorismo la justificación de sus medios no atiende a otro criterio que el de la pura (y máxima) efectividad de sus ataques al orden establecido, para el Estado de derecho la eficacia se mide en términos que no toleran prescindir, en su defensa, de los procedimientos y garantías que lo cualifican como un orden legítimo. Abandonándose sin más a la mera eficacia, el Estado de derecho perdería la cualidad que lo distingue y podría convertirse él mismo, en los casos extremos, en una amenaza para el ciudadano. Nada podría asegurar que, pertrechado el poder público de instrumentos exorbitantes para la persecución del delito, con los que pudiera ignorar o desvirtuar los derechos fundamentales, su acción incontrolada y enteramente libre se desenvolviera finalmente en perjuicio de la libertad de todos.

132. La eficacia del poder público, repito, encuentra una barrera infranqueable en los derechos fundamentales de los ciudadanos, cuyas limitaciones, según prescribe el artículo 52, apartado 1, de la Carta, solo pueden implantarse por ley y respetando su contenido esencial «cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás». [79]

133. Sobre las condiciones en las que, conforme a la sentencia Tele2 Sverige y Watson, sería admisible una conservación *selectiva* de datos, me remito a mis conclusiones del asunto C-520/18. [80]

134. Circunstancias en las que la información disponible en manos de los servicios de seguridad permita abonar la sospecha fundada de la preparación de un atentado terrorista pueden constituir un supuesto legítimo de imposición de la obligación de conservar ciertos datos. Con mayor motivo puede hacerlo la comisión efectiva de un atentado. Si, en este último caso, la perpetración del delito puede ser por sí sola una circunstancia justificativa de la adopción de aquella medida, ante la mera sospecha de un eventual atentado sería necesario que las circunstancias que la fundamentan ofrecieran un grado mínimo de verosimilitud, imprescindible para una ponderación objetiva de los indicios que pueden justificarla.

78 Así lo interpreta, por ejemplo, el Gobierno francés, que ilustra esta afirmación con ejemplos concretos de la utilidad de la conservación generalizada de datos, que permitió la reacción del Estado frente a los graves atentados terroristas padecidos en su país en los últimos años (apartados 107 y 122 a 126 del escrito de observaciones del Gobierno francés).

79 Sentencia de 15 de febrero de 2016, N. (C-601/15 PPU, EU:C:2016:84), apartado 50. Se trata, pues, del difícil equilibrio entre el orden público y la libertad al que ya me he referido y al que aspira por principio toda la normativa de la Unión. Sirva de ejemplo la Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo de 15 de marzo de 2017, relativa a la lucha contra el terrorismo y por la que se sustituye la Decisión marco 2002/475/JAI del Consejo y se modifica la Decisión 2005/671/JAI del Consejo (DO 2017, L 88, p. 6). Al tiempo que recoge en su artículo 20, apartado 1, que los Estados miembros deben garantizar que los responsables de la investigación o enjuiciamiento de delitos de terrorismo «dispongan de instrumentos de investigación eficaces», declara en su considerando vigésimo primero que el recurso a esos instrumentos eficaces «debe ser selectivo y tener en cuenta el principio de proporcionalidad y la naturaleza y gravedad de los delitos investigados, y respetar el derecho a la protección de los datos personales».

80 Puntos 87 a 95.

135. Aunque difícil, no es imposible determinar con precisión y con arreglo a criterios objetivos tanto las categorías de datos cuya conservación se juzgue imprescindible como el círculo de las personas afectadas. Ciertamente, lo más *práctico y eficaz* sería la conservación general e indiscriminada de cuantos datos puedan recabar los proveedores de los servicios de comunicación electrónica, pero ya he señalado que la cuestión no puede dirimirse en términos de *eficacia práctica*, sino de *eficacia jurídica* y en el contexto de un Estado de derecho.

136. Esa labor de determinación es típicamente legislativa, dentro de los límites que la jurisprudencia del Tribunal de Justicia ha marcado. Me remito, de nuevo, a lo que sobre este extremo expongo en mis conclusiones del asunto C-520/18. [81]

3) Acceso a los datos conservados

137. Partiendo, como premisa, de que los operadores han procedido a recopilar los datos de un modo respetuoso con los preceptos de la Directiva 2002/58 y de que su conservación se ha llevado a cabo al amparo de su artículo 15, apartado 1, [82] el acceso de los autoridades competentes a esa información ha de realizarse bajo las condiciones que el Tribunal de Justicia ha exigido y, por mi parte, analizo en las conclusiones del asunto C-520/18, a las que me remito. [83]

138. Por tanto, también en este caso la normativa nacional ha de establecer los requisitos materiales y procedimentales que regulen el acceso de las autoridades competentes a los datos conservados. [84] En el contexto de estos reenvíos prejudiciales, esos requisitos autorizarían el acceso a los datos de las personas que se sospeche que planean, van a cometer, han cometido o puedan estar implicadas en un acto terrorista. [85]

139. Con todo, lo esencial es que, salvo en supuestos de urgencia debidamente justificados, el acceso a los datos en cuestión esté sometido al control previo de un órgano jurisdiccional o de una autoridad administrativa independiente cuya decisión responda a una solicitud motivada de las autoridades competentes. [86] De este modo, allí donde no puede alcanzar el juicio abstracto de la ley se garantiza el juicio *in concreto* de esa autoridad independiente, comprometida por igual con la garantía de la seguridad del Estado y con la defensa de los derechos fundamentales de los ciudadanos.

81 Puntos 100 a 107.

82 En el bien entendido de que se observen las condiciones mencionadas en el apartado 122 de la sentencia Tele2 Sverige y Watson: el Tribunal de Justicia ha recordado que el artículo 15, apartado 1, de la Directiva 2002/58 no admite excepcionar el propio artículo 4, apartados 1 y 1 *bis*, que exige a los proveedores la adopción de medidas que permitan garantizar la protección de los datos conservados contra los riesgos de abuso y contra el acceso ilícito. En este sentido, declaraba que, «[h]abida cuenta de la cantidad de datos conservados, del carácter sensible de esos datos y del riesgo de acceso ilícito a estos, los proveedores de servicios de comunicaciones electrónicas deben garantizar, para asegurar la plena integridad y confidencialidad de esos datos, un nivel particularmente elevado de protección y de seguridad mediante medidas técnicas y de gestión adecuadas. En particular, la normativa nacional debe prever la conservación de los datos en el territorio de la Unión y la destrucción definitiva de los datos al término del período de conservación de estos».

83 Puntos 52 a 60.

84 Sentencia Tele2 Sverige y Watson, apartado 118.

85 *Ibidem*, apartado 119.

86 *Ibidem*, apartado 120.

4) Obligación de conservación de datos que permitan identificar a los autores de contenidos, a la luz de la Directiva 2000/31 (segunda pregunta prejudicial del asunto C-512/18)

140. El tribunal de reenvío alude a la Directiva 2000/31 como punto de referencia para discernir si es posible obligar, a ciertas personas [87] y operadores que ofrecen servicios de comunicación al público, a conservar los datos «que puedan permitir la identificación de quien haya contribuido a crear el contenido o de algunos de los contenidos de los servicios que aquellas prestan, con el fin de que la autoridad judicial pueda requerir, en su caso, la comunicación de los mismos para que se respeten las normas en materia de responsabilidad civil o penal».

141. Coincido con la Comisión en que estaría fuera de lugar examinar la compatibilidad de esa obligación con la Directiva 2000/31, [88] toda vez que el artículo 1, apartado 5, letra b), de esta última excluye de su ámbito de aplicación las «cuestiones relacionadas con servicios de la sociedad de la información incluidas en las Directivas 95/46/CE y 97/66/CE», normas que se corresponden ahora con el Reglamento n.º 2006/679 y con la Directiva 2002/58, [89] cuyos respectivos artículos 23, apartado 1, y 15, apartado 1, deben interpretarse, a mi juicio, en los términos antes expuestos.

2. Sobre la obligación de recopilar en tiempo real datos de tráfico y de localización (segunda pregunta prejudicial del asunto C-511/18)

142. Para el tribunal de reenvío, el artículo L. 851-2 del Código de seguridad interior autoriza, únicamente con fines de prevención del terrorismo, a recopilar, en tiempo real, información acerca de personas previamente identificadas como sospechosas de estar vinculadas con una amenaza terrorista. Del mismo modo, el artículo L. 851-4 de ese Código permite la transmisión en tiempo real, por los operadores, de los datos técnicos relativos a la localización de los equipos terminales.

143. Según el órgano judicial de remisión, estas técnicas no imponen a los proveedores una obligación de conservación suplementaria a la que hace falta para la facturación y la comercialización de sus servicios.

144. Además, a tenor del artículo L. 851-3 del Código de seguridad interior, los operadores de comunicaciones electrónicas y los prestadores de servicios técnicos pueden estar obligados a «aplicar en sus redes tratamientos automatizados de datos destinados, en función de los parámetros establecidos en la autorización, a detectar conexiones que pudieran suponer una amenaza terrorista». Esta técnica no comporta una conservación generalizada e indiferenciada de datos y persigue recopilar, durante un tiempo limitado, aquellos datos de conexión que pudieran estar relacionados con una infracción de carácter terrorista.

145. A mi entender, las condiciones exigibles para el acceso a los datos personales conservados deben aplicarse igualmente al acceso en tiempo real a los datos generados en el curso de las comunicaciones electrónicas. Me remito, pues, a lo dicho sobre ese particular. Que se trate de datos conservados o de datos obtenidos al instante es irrelevante, pues en ambos casos se toma conocimiento de datos personales, sin que importe que sean pretéritos o actuales.

87 Las que «almacenan […] 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 esos servicios […]».

88 Esta Directiva la menciona, en términos genéricos y sin precisar ningún precepto, el tribunal de reenvío en la segunda pregunta del asunto C-512/18.

89 Apartados 112 y 113 del escrito de observaciones de la Comisión.

146. En concreto, si el acceso en tiempo real fuera consecuencia de conexiones detectadas por obra de un tratamiento automatizado, como el recogido en el artículo L. 851-3 del Código de seguridad interior, se impone que los modelos y criterios preestablecidos para ese tratamiento sean específicos, fiables y no discriminatorios, de manera que faciliten la identificación de individuos sobre los que quepa abrigar una sospecha razonable de participación en actividades terroristas. [90]

3. Sobre la obligación de informar a los afectados (tercera pregunta prejudicial del asunto C-511/18)

147. El Tribunal de Justicia ha afirmado que las autoridades a las que se conceda el acceso a los datos han de informar de esta circunstancia a las personas afectadas, siempre que no se comprometan las investigaciones en curso. El motivo de ese deber estriba en que dicha información es necesaria para que aquellas personas puedan ejercer su derecho a la tutela judicial efectiva, expresamente citado en el artículo 15, apartado 2, de la Directiva 2002/58, en caso de vulneración de sus derechos. [91]

148. El Conseil d'État (Consejo de Estado) desea saber, con su tercera pregunta en el asunto C-511/18, si esa exigencia de información es en todo caso inexcusable o si cabe dispensarla cuando se hayan previsto otras garantías, como las que describe en su auto de remisión.

149. De acuerdo con la exposición del tribunal de reenvío, [92] las mencionadas garantías se cifran en la posibilidad de que quienes deseen comprobar si una técnica de información ha sido aplicada de manera ilegal se dirijan al propio Conseil d'État (Consejo de Estado). Este órgano podría llegar, en su caso, a anular la autorización de la medida y ordenar la destrucción de lo recopilado, en el seno de un procedimiento que no contempla el principio de contradicción habitual de los procesos jurisdiccionales.

150. El órgano de reenvío considera que esa normativa no vulnera el derecho a la tutela judicial efectiva. Creo, sin embargo, que así podría admitirse, en teoría, para quienes decidan comprobar si son objeto de una operación de inteligencia. Por el contrario, no se respeta aquel derecho si, a quienes, siendo o habiendo sido objeto de esa operación, no se les advierte de esa circunstancia y, por tanto, no pueden plantearse siquiera si sus derechos han sido o no conculcados.

151. Las garantías jurisdiccionales a las que se refiere el órgano judicial de remisión parecen estar condicionadas a la iniciativa de quien sospeche ser objeto de una recopilación de información sobre su persona. Sin embargo, el acceso a la jurisdicción para la defensa de sus derechos debe ser efectivo para todos, lo que comporta que quien haya soportado un tratamiento de sus datos personales ha de tener la posibilidad de cuestionar judicialmente la legalidad de dicho tratamiento y, en consecuencia, se le debe notificar su existencia.

152. Ciertamente, según se desprende de la información facilitada, la acción de la justicia puede desencadenarse de oficio o en virtud de denuncia administrativa, pero debe darse al afectado, en todo caso, la posibilidad de ser él mismo quien la incoe, para lo que es necesario que se le revele que sus datos personales han sido objeto de determinado tratamiento. No puede fiarse la defensa de sus derechos a la circunstancia de que llegue a tener conocimiento de ese tratamiento por terceros o por sus propios medios.

153. Así pues, en la medida en que no se comprometa el curso de las investigaciones para las que se ha concedido el acceso a los datos conservados, a la persona afectada se le debe comunicar dicho acceso.

90 Sentencia Digital Rights, apartado 59.

91 Sentencia Tele2 Sverige y Watson, apartado 121.

92 Apartados 8 a 11 del auto de remisión.

154. Distinto, es que, interesada la acción de la justicia por la persona afectada, una vez que se le ha hecho saber el acceso a sus datos, el subsiguiente procedimiento jurisdiccional se acomode a las exigencias de confidencialidad y de reserva inherentes a la fiscalización de la acción de los poderes públicos en ámbitos sensibles como el de la seguridad y la defensa del Estado. Esa cuestión es, sin embargo, ajena a estos reenvíos, de manera que no procede, a mi juicio, que el Tribunal de Justicia se pronuncie al respecto.

V. Conclusión

155. A tenor de lo expuesto, sugiero al Tribunal de Justicia responder al Conseil d'État (Consejo de Estado, Francia) en los siguientes términos:

«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, debe interpretarse en el sentido de que:

1) Se opone a una normativa nacional que, en un contexto caracterizado por amenazas graves y persistentes para la seguridad nacional, en especial por el riesgo terrorista, impone a los operadores y prestadores de los servicios de comunicaciones electrónicas la obligación de conservar, de modo general e indiferenciado, los datos de tráfico y de localización de todos los abonados, así como los datos que permitan identificar a los creadores de los contenidos ofrecidos por los proveedores de dichos servicios.

2) Se opone a una normativa nacional que no instaura la obligación de informar a las personas afectadas acerca del tratamiento de sus datos personales llevado a cabo por las autoridades competentes, salvo que esa comunicación comprometa la acción de dichas autoridades.

3) No se opone a una normativa nacional que permite recopilar en tiempo real los datos de tráfico y localización de personas singulares, en la medida en que esas actuaciones se realicen con arreglo a los procedimientos establecidos para el acceso a los datos personales legítimamente conservados y con las mismas garantías».