Recopilación de la Jurisprudencia

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

Asunto C-623/17

Privacy International
contra
Secretary of State for Foreign and Commonwealth Affairs,
Secretary of State for the Home Department,
Government Communications Headquarters,
Security Service,
Secret Intelligence Service

[Petición de decisión prejudicial planteada por el Investigatory Powers Tribunal (Tribunal de los poderes de investigación, Reino Unido)]

«Cuestión prejudicial — Tratamiento de datos de carácter personal y protección de la vida privada en el sector de las comunicaciones electrónicas — Directiva 2002/58/CE — Ámbito de aplicación — Artículo 1, apartado 3 — Artículo 15, apartado 3 — Carta de los Derechos Fundamentales de la Unión Europea — Artículos 7, 8, 51 y 52, apartado 1 — Artículo 4 TUE, apartado 2 — Transmisión generalizada e indiferenciada a los servicios de seguridad de datos de conexión de los usuarios de un servicio de comunicaciones electrónicas»

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 los Derechos Fundamentales de la Unión Europea.

– 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]

– 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.

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).

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

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

3. Determinados órganos jurisdiccionales de los Estados miembros han puesto de relieve esa misma preocupación en cuatro reenvíos prejudiciales,[7] cuyas conclusiones presento con esta misma fecha.

4. Los cuatro asuntos plantean, 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, habría 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

5. Me remito al apartado correspondiente de mis conclusiones en los asuntos C-511 y C-512/18.

B. Derecho nacional (aplicable al supuesto litigioso)

1. Telecommunications Act 1984[11]

6. Con arreglo al artículo 94, el secretario de Estado puede dirigir a un operador de una red pública de comunicaciones electrónicas las instrucciones generales o específicas que considere necesarias en interés de la seguridad nacional o de las relaciones con el Gobierno de un país o territorio situado fuera del Reino Unido.

2. Data Retention and Investigatory Powers Act 2014[12]

7. El artículo 1 establece:

«(1) El secretario de Estado puede, mediante una orden de conservación, requerir a un operador de telecomunicaciones públicas la conservación de datos de comunicación relevantes, si considera que dicho requerimiento es necesario y proporcionado respecto de uno o varios de los objetivos contemplados en los apartados (a) a (h) del artículo 22, apartado 2, de la Regulation of Investigatory Powers Act 2000 [(Ley de 2000 sobre la regulación de los poderes de investigación; en lo sucesivo, «RIPA»)].

7 Además de este, se trata de los asuntos C-511/18 y C-512/18, La Quadrature du Net y otros, 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.

11 Ley de 1984 sobre las telecomunicaciones; en lo sucesivo, «Ley de 1984».

12 Ley de 2014 sobre la conservación de datos y los poderes de investigación; en lo sucesivo, «DRIPA».

(2) Una orden de conservación puede:

(a) referirse a un operador en particular o a todo tipo de operadores,

(b) imponer la conservación de todos los datos o de toda categoría de datos,

c) precisar el período o los períodos durante los que deben conservarse los datos,

(d) comportar otras exigencias o restricciones en relación con la conservación de datos,

(e) prever disposiciones diferentes para fines diferentes,

(f) referirse a datos que existan o no en la fecha en la que se adopte o entre en vigor la orden de conservación.

(3) El secretario de Estado puede, por vía de reglamento, adoptar más disposiciones relativas a la conservación de los datos pertinentes relativos a las comunicaciones.

(4) Estas disposiciones pueden referirse, en particular, a:

(a) las exigencias previas a la adopción de la orden de conservación,

(b) el período máximo durante el que deben conservarse los datos en virtud de una orden de conservación,

(c) el contenido, la adopción, la entrada en vigor, el reexamen, la modificación o la revocación de una orden de conservación,

(d) la integridad, la seguridad o la protección de los datos conservados en aplicación del presente artículo, el acceso a los datos, así como su divulgación o destrucción,

(e) el cumplimiento de las exigencias o restricciones pertinentes o la verificación de la conformidad a las mismas,

(f) un código de buenas prácticas relativas a las exigencias, restricciones o poderes pertinentes,

(g) el reembolso por el secretario de Estado (bajo ciertas condiciones o no) de los costes en que hayan incurrido los operadores de telecomunicaciones públicas para cumplir con las exigencias o restricciones pertinentes,

[…]

(5) El período máximo previsto en aplicación del apartado 4, letra b), no debe exceder de 12 meses a contar desde la fecha indicada en relación con los datos a los que conciernen los reglamentos a los que se refiere el apartado 3.

(6) Un operador de telecomunicaciones públicas que conserve datos pertinentes relativos a las comunicaciones en aplicación del presente artículo no puede divulgar esos datos a menos que:

(a) los divulgue de conformidad con:

(i) el capítulo 2 de la parte 1 de la [RIPA] o

(ii) una decisión judicial o cualquier otra autorización o mandato judiciales, o que

(b) esté previsto por los reglamentos a los que se refiere el apartado 3.

(7) El secretario de Estado puede, por vía reglamentaria, adoptar disposiciones respecto de cualesquiera de las disposiciones adoptadas (o susceptibles de ser adoptadas) en aplicación del apartado 4, letras (d) a (g) o del apartado 6, en relación con los datos relativos a las comunicaciones conservadas por proveedores de servicios de telecomunicaciones en aplicación de un código de buenas prácticas en virtud del artículo 102 de la Ley de 2001 sobre la lucha antiterrorista, la criminalidad y la seguridad [Anti-terrorism, Crime and Security Act 2001]».

3. RIPA

8. El artículo 21 señala:

«[…]

(4) En el presente capítulo se entiende por "datos relativos a las comunicaciones" cualesquiera de las nociones siguientes:

(a) todo dato relativo al tráfico comprendido en, o adjunto a, una comunicación (por el expedidor o de otro modo) a los fines de cualquier servicio postal o sistema de telecomunicación por medio del que se transmite o puede ser transmitida,

(b) toda información que no incluya ningún contenido de una comunicación [exceptuada toda información comprendida en la letra (a)] y que se refiera a la utilización efectuada por cualquier persona:

(i) de todo servicio postal o de telecomunicación; o

(ii) en relación con el suministro o la utilización por cualquier persona de cualquier servicio de telecomunicaciones, de cualquier parte de un sistema de telecomunicaciones,

(c) toda información no comprendida en las letras (a) o (b) poseída u obtenida, en relación con las personas destinatarias del servicio, por una persona que suministre un servicio postal o un servicio de telecomunicaciones.

[…]

(6) En esta sección, el concepto "dato relativo al tráfico", en relación con cualquier comunicación se refiere a:

(a) todo dato identificador o susceptible de identificar a toda persona, aparato o localización hacia la cual, o a partir de la cual, se transmite o puede transmitirse una comunicación;

(b) todo dato identificador o seleccionador, o susceptible de identificar o seleccionar el equipo por el que se transmite o puede ser transmitida la comunicación;

(c) todo dato que comprenda señales para el accionamiento del aparato utilizado en un sistema de comunicación a los fines de la transmisión de toda comunicación; y

(d) todo dato identificador de los datos comprendidos en o adjuntos a una comunicación particular u otros datos en tanto que comprendidos en o adjuntos a una comunicación particular.

[…]»

9. El artículo 22 prescribe:

«(1) Este artículo se aplica cuando una persona responsable a los fines del presente capítulo considera que es necesario, por las razones enumeradas en el apartado 2 del presente artículo, obtener todo dato de comunicación.

(2) Es necesario por razones comprendidas en el presente apartado obtener los datos de comunicación si son necesarios

(a) en interés de la seguridad nacional,

(b) a los fines de la prevención o la detección de la criminalidad o de la prevención de trastornos del orden público,

(c) en el interés del bienestar económico del Reino Unido siempre que esos intereses sean igualmente pertinentes para los intereses de la seguridad nacional,

(d) en el interés de la seguridad pública,

(e) a los fines de la protección de la salud pública,

(f) a los fines de la evaluación de la imposición o recaudación de todo impuesto, derecho, canon u otra imposición, contribución o carga debida a la administración pública,

(g) a los fines de la prevención, en caso de urgencia, de decesos, lesiones o todo perjuicio para la salud física o mental de una persona física o de la atenuación de toda lesión o perjuicio para la salud física o mental de una persona física,

(h) a cualquier otro fin [no comprendido en las letras (a) a (g)] determinado en una orden cursada por el secretario de Estado en virtud del artículo 22, apartado 2, letra (h), de la [DRIPA].

(4) A reserva del apartado 5, la persona responsable, cuando le parezca que un operador de telecomunicaciones o un operador postal está en posesión de datos, podría estarlo o podría ser capaz de estarlo, puede exigir al operador de telecomunicación o al operador postal que:

(a) obtenga los datos, si aún no los tiene, y

(b) divulgue, en todo caso, todos los datos en su posesión o que ha obtenido después.

(5) La persona responsable no debe autorizar con arreglo al apartado 3 ni requerir en virtud del apartado 4, salvo si considera que la obtención de los datos en cuestión que resultan de un comportamiento autorizado o exigido en virtud de una autorización o de una demanda es proporcionado con el fin perseguido por la obtención de los datos».

10. A tenor del artículo 65, cabe recurrir ante el Investigatory Powers Tribunal (Tribunal de los poderes de investigación, Reino Unido) si hay razón para pensar que se han obtenido datos de manera inapropiada.

II. Hechos y cuestiones prejudiciales

11. Según el tribunal *a quo*, el litigio principal versa sobre la adquisición y el uso por las United Kingdom Security and Intelligence Agencies (Agencias de seguridad y de inteligencia del Reino Unido; en lo sucesivo, «ASI») de datos objeto de comunicación masiva.

12. Estos datos se refieren a «quién» usa el teléfono e internet, y a «cuándo, dónde, cómo y con quién» los usa. Comprenden la ubicación de los teléfonos móviles y fijos desde los que se realizan o reciben llamadas, así como de los ordenadores desde los que se accede a internet. No incluyen el contenido de las comunicaciones, que únicamente puede obtenerse por orden judicial.

13. La demandante en el proceso principal (Privacy International, organización no gubernamental de defensa de los derechos humanos) ha entablado una acción ante el órgano jurisdiccional remitente, por entender que la adquisición y la utilización de los mencionados datos por las ASI vulneran el derecho al respeto de la vida privada consagrado en el artículo 8 del Convenio Europeo de Derechos Humanos (en lo sucesivo, «CEDH») y son contrarios al derecho de la Unión.

14. Las autoridades demandadas [13] alegan que el ejercicio de su competencia en este ámbito es legítimo y esencial, en particular, para proteger la seguridad nacional.

15. Según las informaciones contenidas en el auto de remisión, al amparo de las instrucciones emitidas por el secretario de Estado conforme al artículo 94 de la Ley de 1984, las ASI reciben los datos de comunicación masiva a través de los operadores de las redes públicas de comunicaciones electrónicas.

16. Dichos datos incluyen información sobre el tráfico y la ubicación, así como sobre las actividades sociales, comerciales y financieras, las comunicaciones y los viajes de los usuarios. Las ASI conservan esos datos, una vez en su poder, de manera segura, empleando técnicas (por ejemplo, el filtrado y la agregación) generalizadas, esto es, no dirigidas a objetivos específicos y conocidos.

17. El órgano jurisdiccional remitente considera probado que esas técnicas son esenciales para la labor de las ASI en la lucha contra las amenazas graves a la seguridad pública, en especial, el terrorismo, el espionaje y la proliferación nuclear. La capacidad de adquirir y usar los datos, por parte de las ASI, es clave para proteger la seguridad nacional del Reino Unido.

18. Para el tribunal de reenvío, las medidas controvertidas se ajustan al derecho interno y al artículo 8 del CEDH. Duda, sin embargo, sobre su compatibilidad con el derecho de la Unión, a la vista de la sentencia Tele2 Sverige y Watson.

19. En este contexto, dicho órgano jurisdiccional eleva al Tribunal de Justicia las siguientes preguntas prejudiciales:

«1) A la luz del artículo 4 TUE y del artículo 1, apartado 3, de la Directiva 2002/58 […], ¿tiene cabida en el derecho de la Unión y en la Directiva [2002/58] un requisito por el cual un proveedor de redes de comunicación electrónica debe facilitar datos objeto de comunicaciones masivas a las Agencias de Seguridad e Inteligencia (ASI) de un Estado miembro de acuerdo con las instrucciones recibidas del secretario de Estado?

2) En caso de respuesta afirmativa a la primera cuestión, ¿se aplican los Requisitos Watson, [14] u otros requisitos además de los impuestos por el CEDH, a las referidas instrucciones del Secretario de Estado? En caso afirmativo, ¿cómo y en qué medida deben aplicarse dichos requisitos, habida cuenta de la necesidad esencial de las ASI de usar técnicas de adquisición y tratamiento masivo automatizado para proteger la seguridad nacional, y de la circunstancia de que tal capacidad, en caso de ser conforme con el CEDH, puede sufrir un menoscabo significativo como consecuencia de esos requisitos?»

13 El Secretary of State for Foreign and Commonwealth Affairs (secretario de Estado para Asuntos Exteriores y de la Commonwealth), el Secretary of State for the Home Department (secretario de Estado para Asuntos de Interior) y las tres ASI del Reino Unido, a saber, la Government Communications Headquarters (Sede de Comunicaciones del Gobierno; GCHQ), el Security Service (Servicio de Seguridad; MI5), y el Secret Intelligence Service (Servicio Secreto de Inteligencia; MI6).

14 *Id est*, la jurisprudencia establecida en la sentencia Tele2 Sverige y Watson.

20. El tribunal de remisión contextualiza sus preguntas en estos términos:

«a) la capacidad [de las ASI] para usar determinados [datos de comunicación masiva] que se les han suministrado es esencial para proteger la seguridad nacional del Reino Unido, en particular, en los ámbitos de lucha contra el terrorismo, el contraespionaje y la proliferación nuclear;

b) un objetivo esencial del uso que las ASI hacen de [esos datos] consiste en descubrir amenazas hasta entonces desconocidas para la seguridad nacional, mediante técnicas masivas generales basadas en la acumulación de [esos datos] en un único lugar. Su utilidad principal reside en la identificación y el desarrollo de objetivos de forma ágil y en la obtención de una base de actuación en caso de amenaza inminente;

c) no se exige a los proveedores de redes de comunicación electrónica que conserven los mencionados datos (más allá de los plazos obligatorios), que quedan exclusivamente en poder del Estado (las ASI);

d) el órgano jurisdiccional nacional considera que (sin perjuicio de determinadas cuestiones reservadas) las salvaguardas que rodean el uso de [esos datos] por las ASI cumplen los requisitos establecidos en el CEDH; y

e) el órgano jurisdiccional nacional estima que la imposición de los requisitos precisados en la sentencia [Tele2 Sverige y Watson], en caso de ser aplicables, redundaría en perjuicio de las medidas adoptadas por las ASI para salvaguardar la seguridad nacional y, en consecuencia, pondría en riesgo la seguridad nacional del Reino Unido».

III. Procedimiento ante el Tribunal de Justicia

21. La cuestión prejudicial se registró en el Tribunal de Justicia el 31 de octubre de 2017.

22. Han depositado observaciones escritas los Gobiernos alemán, belga, británico, checo, chipriota, español, estonio, francés, húngaro, irlandés, letón, neerlandés, noruego, polaco, portugués y sueco, así como la Comisión.

23. El 9 de septiembre de 2019 tuvo lugar una vista pública, celebrada conjuntamente con las de los asuntos C-511/18, C-512/18, y C-520/18, en la que comparecieron las partes de los cuatro reenvíos prejudiciales, los Gobiernos antes citados, así como la Comisión y el Supervisor europeo para la protección de datos personales.

IV. Análisis

A. Sobre el ámbito de aplicación de la Directiva 2002/58 y la exclusión de la seguridad nacional (primera pregunta prejudicial)

24. En las conclusiones que con esta misma fecha presento en los asuntos C-511/18 y C-512/18, explico los motivos por los que, a mi juicio, 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 esta tesis que las obligaciones se impongan a los proveedores por razones de seguridad nacional». [15]

15 Conclusiones de los asuntos C-511/18 y C-512/18, punto 42.

25. Al desarrollar mis argumentos, abordo la incidencia de las sentencias del Tribunal de Justicia de 30 de mayo de 2006, Parlamento/Consejo y Comisión,[16] y Tele2 Sverige y Watson, auspiciando una interpretación integradora de ambas.[17]

26. En esas mismas conclusiones, una vez afirmada la aplicabilidad de la Directiva 2002/58, examino la exclusión de la seguridad nacional que consta en ella y la incidencia del artículo 4 TUE, apartado 2.[18]

27. Sin perjuicio de lo que a continuación expondré, me remito a lo ya dicho en las reiteradas conclusiones y en las del asunto C-520/18.

1. La aplicación de la Directiva 2002/58 en este asunto

28. A tenor de las normas controvertidas en este litigio, los proveedores de servicios de comunicaciones electrónicas son destinatarios de una obligación que implica, además de su conservación, un tratamiento de los datos que poseen a causa del servicio que prestan a los usuarios de las redes públicas de comunicaciones de la Unión.[19]

29. En efecto, los mencionados operadores han de transmitir, obligatoriamente, aquellos datos a las ASI. Lo que aquí se suscita es si el artículo 15, apartado 1, de la Directiva 2002/58 consiente que esa transmisión, dado su objetivo, se excluya, sin más, del derecho de la Unión.

30. En mi opinión, no es así. La conservación de los referidos datos seguida de su ulterior transmisión se puede calificar de tratamiento de datos personales realizado por los proveedores de servicios de telecomunicaciones electrónicas, por lo que se inscriben con naturalidad en el ámbito de aplicación de la Directiva 2002/58.

31. Las razones de seguridad nacional no pueden anteponerse a esa constatación, como sugiere el órgano judicial remitente, con la consecuencia de que la obligación controvertida no quedaría comprendida en el ámbito de aplicación del derecho de la Unión. A mi parecer, repito, se impone a los proveedores un tratamiento de datos, en relación con la prestación de servicios de comunicaciones electrónicas disponibles al público en las redes públicas de comunicaciones de la Unión, que es justamente el ámbito de la Directiva 2002/58, según prescribe su artículo 3, apartado 1.

32. Sentada esta premisa, el debate se desplaza no ya a las actividades de las ASI (que, como antes he advertido, podrían situarse extramuros del derecho de la Unión si no afectasen a los operadores de comunicaciones electrónicas), sino a la conservación y a la ulterior transmisión de los datos en poder de dichos operadores. Desde esta perspectiva, lo que entra en juego son los derechos fundamentales garantizados por la Unión.

33. El factor clave para dirimir ese debate es, una vez más, el deber de conservación generalizada e indiferenciada de los datos cuyo acceso se facilita a las autoridades públicas.

16 Asuntos C-317/04 y C-318/04, EU:C:2006:346.

17 Conclusiones de los asuntos C-511/18 y C-512/18, puntos 44 a 76.

18 *Ibidem*, puntos 77 a 90.

19 En virtud del artículo 2 de la Directiva 2002/58, se aplican, a los efectos de esa Directiva, las definiciones que figuran en la Directiva 95/46. Con arreglo al artículo 2, letra b), de esta última, se entiende por «tratamiento de datos personales» «cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, *comunicación por transmisión*, difusión o cualquier otra *forma que facilite el acceso a los mismos*, cotejo o interconexión, así como su bloqueo, supresión o destrucción» (cursiva añadida).

2. La apelación a la seguridad nacional

34. Como en este asunto el órgano de reenvío hace especial hincapié en la actividad de las ASI que afectan a la seguridad nacional, me permito reproducir algunos de los puntos de mis conclusiones de esta misma fecha en los asuntos C-511/18 y C-512/18, sobre este extremo:

«77. La seguridad nacional […] es objeto de una doble consideración en la Directiva 2002/58. Por una parte, 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 otra parte, 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.

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 citar 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". [...]

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.

[…]

82. Estimo […] que puede valer de orientación el criterio de la Decisión marco 2006/960/JAI, [...] 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. [...]

[…]

84. Hay […] una continuidad entre la Directiva 95/46 y la Directiva 2002/58 en cuanto 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 [el] considerando [décimo primero de la Directiva 2002/58] 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.

[…]

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 preciso 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».

3. Las consecuencias de aplicar en este asunto la sentencia Tele2 Sverige y Watson

35. El órgano judicial de reenvío se ha centrado en la interpretación hecha por el Tribunal de Justicia en la sentencia Tele2 Sverige y Watson, exponiendo las dificultades que, en su opinión, comportaría su aplicación a este asunto.

36. La sentencia Tele2 Sverige y Watson indicó, en efecto, las condiciones que ha de satisfacer una normativa nacional que instaure la obligación de conservar datos de tráfico y de localización, para su ulterior acceso por las autoridades públicas.

37. Al igual que en los asuntos C-511/18 y C-512/18, y por análogos motivos, considero que las normas nacionales sobre las que versa este reenvío no se atienen a las condiciones recogidas en la sentencia Tele2 Sverige y Watson, pues implican una conservación generalizada e indiferenciada de datos personales que facilita un detallado relato de la vida de las personas afectadas, durante un amplio período de tiempo.

38. En las conclusiones de aquellos dos asuntos me planteo si sería posible matizar o completar la doctrina expuesta en dicha sentencia, dadas sus consecuencias para la lucha contra el terrorismo o para la protección del Estado frente a otras amenazas análogas contra la seguridad nacional.

39. Me permito también reproducir a continuación algunos de los puntos de aquellas conclusiones, en los que, básicamente, sostengo que, siendo posible matizar la mencionada doctrina, procede confirmarla en lo sustancial:

«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 […] 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. […]

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, [...] el acceso de las 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.

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. [...] 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. [...]

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. [...] 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».

B. Sobre la segunda cuestión prejudicial

40. El órgano judicial de reenvío formula su segunda pregunta por si la contestación a la primera fuera afirmativa. En tal caso, querría saber qué «otros requisitos además de los impuestos por el CEDH» o los que derivan de la sentencia Tele2 Sverige y Watson deberían exigirse.

41. Asevera, en este sentido, que la imposición de las condiciones de la sentencia Tele2 Sverige y Watson, «redundaría en perjuicio de la eficacia de las medidas adoptadas por las ASI para salvaguardar la seguridad nacional».

42. Como la respuesta que sugiero a la primera pregunta es negativa, no resulta indispensable abordar la segunda. Esta última, como el propio tribunal de reenvío destaca, está supeditada a que se declaren compatibles con el derecho de la Unión «las técnicas de adquisición y tratamiento masivo automatizado» de los datos personales de todos los usuarios del Reino Unido, que los operadores de los servicios de comunicaciones electrónicas habrían de transmitir a las ASI.

43. Si el Tribunal de Justicia estimara imprescindible responder a la segunda pregunta, entiendo que debería corroborar las aludidas condiciones de la sentencia Tele2 Sverige y Watson en relación con:

– la proscripción del acceso generalizado a los datos;

– la necesidad de autorización previa de un juez o de una autoridad independiente para legitimar ese acceso;

– la obligación de informar a los afectados, salvo si así se comprometiera la eficacia de la medida;

– la conservación de los datos dentro de la Unión.

44. Bastaría, repito, confirmar esas condiciones, de obligada aplicación, por las razones que he expuesto en las conclusiones de los asuntos C-511/18 y C-512/18 y C-520/18, sin necesidad de implantar «otras» adicionales, en el sentido al que se refiere el tribunal de reenvío.

V. Conclusión

45. En virtud de todo lo anterior, propongo al Tribunal de Justicia responder al Investigatory Powers Tribunal (Tribunal de los poderes de investigación, Reino Unido) en estos términos:

«El artículo 4 TUE y el artículo 1, apartado 3, 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), deben interpretarse en el sentido de que se oponen a una normativa nacional que imponga a un proveedor de redes de comunicación electrónica la obligación de facilitar a las agencias de seguridad e inteligencia de un Estado miembro los "datos objeto de comunicaciones masivas" que implican su previa recopilación generalizada e indiferenciada».

Con carácter subsidiario:

«El acceso, por parte de las agencias de seguridad e inteligencia de un Estado miembro, a los datos transmitidos por los proveedores de redes de comunicación electrónica debe ajustarse a las condiciones establecidas en la sentencia de 21 de diciembre de 2016, Tele2 Sverige y Watson (C-203/15 y C-698/15, EU:C:2016:970)».