Recopilación de la Jurisprudencia

CONCLUSIONES DEL ABOGADO GENERAL
M. CAMPOS SÁNCHEZ-BORDONA
presentadas el 12 de mayo de 2016 [1]

Asunto C-582/14

Patrick Breyer
contra
Bundesrepublik Deutschland[Petición de decisión prejudicial

planteada por el Bundesgerichtshof (Tribunal Supremo Civil y Penal, Alemania)]

«Tratamiento de datos de carácter personal — Directiva 95/46/CE — Artículo 2, letra a), y artículo 7, letra f) — Concepto de "datos de carácter personal" — Direcciones IP — Conservación por un proveedor de servicios de medios electrónicos — Normativa nacional que no permite tener en cuenta el interés legítimo perseguido por el responsable del tratamiento»

1. Una dirección de protocolo de Internet (en adelante, «dirección IP») es una secuencia de números binarios que, asignada a un dispositivo (un ordenador, una tableta, un teléfono inteligente), lo identifica y le permite acceder a la red de comunicaciones electrónicas. El dispositivo, para conectarse a Internet, ha de emplear la secuencia numérica proporcionada por los proveedores del servicio de acceso a la red. La dirección IP se transmite al servidor donde está almacenada la página web objeto de consulta.

2. En particular, los proveedores de acceso a la red (por lo general, las compañías telefónicas) atribuyen a sus clientes las denominadas «direcciones IP dinámicas», de manera temporal, para cada conexión a Internet, y las cambian con ocasión de las conexiones posteriores. Esas mismas compañías llevan un registro en el que consta qué dirección IP han adjudicado, en cada momento, a un determinado dispositivo. [2]

3. Los titulares de los sitios web a los que se accede mediante las direcciones IP dinámicas también suelen mantener registros en los que constan qué páginas se han consultado, cuándo y desde qué dirección IP dinámica. Esos registros pueden, técnicamente, conservarse sin límites temporales, una vez terminada la conexión a Internet de cada usuario.

4. Una dirección IP dinámica, por sí sola, no basta para que el prestador de servicios identifique al usuario de su página web. Sin embargo, podrá hacerlo si combina la dirección IP dinámica con otros datos adicionales en manos del proveedor de acceso a la red.

1 — Lengua original: español.

2 — El artículo 5 de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE (DO 2006, L 105, p. 54), imponía, entre otras obligaciones, la de conservar, con fines de investigación, detección y sanción de las infracciones graves, «la fecha y hora de la conexión y desconexión del servicio de acceso a Internet, […] así como la dirección del Protocolo Internet, ya sea dinámica o estática, asignada por el proveedor de acceso a Internet a una comunicación, así como la identificación de usuario del abonado o del usuario registrado».

5. En el litigio se debate si las direcciones IP dinámicas son un dato de carácter personal, en el sentido del artículo 2, letra a), de la Directiva 95/46/CE.[3] La respuesta exige conocer, previamente, qué relevancia tiene, a esos efectos, el que los datos adicionales necesarios para la identificación del usuario no estén en posesión del titular del sitio web, sino de un tercero (en concreto, del proveedor del servicio de acceso a la red).

6. Es una cuestión inédita para el Tribunal de Justicia, pues, en el apartado 51 de la sentencia Scarlet Extended,[4] declaró que las direcciones IP «son datos protegidos de carácter personal, ya que permiten identificar concretamente a tales usuarios», pero en un contexto en el que la recogida y la identificación de las direcciones IP las realizaba el proveedor de acceso a la red,[5] no un proveedor de contenidos, como es ahora el caso.

7. Si las direcciones IP dinámicas fueran, para el prestador de servicios de Internet, datos de carácter personal, habría de examinarse, acto seguido, si su tratamiento se incluye en el ámbito de la Directiva 95/46.

8. Es posible que, aun siendo datos personales, no gocen de la protección derivada de la Directiva 95/46 si, por ejemplo, la finalidad de su tratamiento fuera el ejercicio de actuaciones penales contra eventuales atacantes de la página web. En esta hipótesis, la Directiva 95/46 no resulta aplicable, con arreglo al artículo 3, apartado 2, primer guion.

9. Hay que dilucidar, además, si el prestador de servicios que registra las direcciones IP dinámicas cuando un usuario accede a sus páginas web (en este asunto, la República Federal de Alemania) actúa como poder público o, más bien, como un particular.

10. Si fuera aplicable la Directiva 95/46, habría que precisar, por último, hasta qué punto su artículo 7, letra f), es compatible con una normativa nacional que restringe el alcance de una de las condiciones establecidas en él para justificar el tratamiento de datos de carácter personal.

I. Marco normativo

A. *Derecho de la Unión*

11. El considerando 26 de la Directiva 95/46 es del siguiente tenor:

«(26) Considerando que los principios de la protección deberán aplicarse a cualquier información relativa a una persona identificada o identificable; que, para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona; que los principios de la protección no se aplicarán a aquellos datos hechos anónimos de manera tal que ya no sea posible identificar al interesado; que los códigos de conducta con arreglo al artículo 27 pueden constituir un elemento útil para proporcionar indicaciones sobre los medios gracias a los cuales los datos pueden hacerse anónimos y conservarse de forma tal que impida identificar al interesado».

3 — 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).

4 — Sentencia de 24 de noviembre de 2011 (C-70/10, EU:C:2011:771), apartado 51.

5 — Así sucedía también en la sentencia de 19 de abril de 2012, Bonnier Audio y otros (C-461/10, EU:C:2012:219), apartados 51 y 52.

12. Conforme al artículo 1 de la Directiva 95/46:

«1. Los Estados miembros garantizarán, con arreglo a las disposiciones de la presente Directiva, la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales.

2. Los Estados miembros no podrán restringir ni prohibir la libre circulación de datos personales entre los Estados miembros por motivos relacionados con la protección garantizada en virtud del apartado 1.»

13. Según el artículo 2 de la Directiva 95/46:

«A efectos de la presente Directiva, se entenderá por:

a) "datos personales": toda información sobre una persona física identificada o identificable (el "interesado"); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social;

b) "tratamiento de datos personales" ("tratamiento"): 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;

[…]

d) "responsable del tratamiento": la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que solo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el derecho nacional o comunitario;

[…]

f) "tercero": la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento;

[…]».

14. Bajo la rúbrica «Ámbito de aplicación», el artículo 3 de la Directiva 95/46 prescribe:

«1. Las disposiciones de la presente Directiva se aplicarán 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. Las 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, como las previstas por las disposiciones de los títulos V y VI del Tratado de la Unión Europea 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;

[…]».

15. El capítulo II de la Directiva 95/46, referido a las «Condiciones generales para la licitud del tratamiento de datos personales», se abre con el artículo 5, de acuerdo con el que «los Estados miembros precisarán, dentro de los límites de las disposiciones del presente capítulo, las condiciones en que son lícitos los tratamientos de datos personales».

16. Con arreglo al artículo 6 de la Directiva 95/46:

«1. Los Estados miembros dispondrán que los datos personales sean:

a) tratados de manera leal y lícita;

b) recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando los Estados miembros establezcan las garantías oportunas;

c) adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente;

d) exactos y, cuando sea necesario, actualizados; deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados;

e) conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente. Los Estados miembros establecerán las garantías apropiadas para los datos personales archivados por un período más largo del mencionado, con fines históricos, estadísticos o científicos.

2. Corresponderá a los responsables del tratamiento garantizar el cumplimiento de lo dispuesto en el apartado 1.»

17. Según el artículo 7 de la Directiva 95/46:

«Los Estados miembros dispondrán que el tratamiento de datos personales solo pueda efectuarse si:

a) el interesado ha dado su consentimiento de forma inequívoca, o

b) es necesario para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado, o

c) es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, o

d) es necesario para proteger el interés vital del interesado, o

e) es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos, o

f) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva.»

18. A tenor del artículo 13 de la Directiva 95/46:

«1. Los Estados miembros podrán adoptar medidas legales para limitar el alcance de las obligaciones y los derechos previstos en el apartado 1 del artículo 6, en el artículo 10, en el apartado 1 del artículo 11, y en los artículos 12 y 21 cuando tal limitación constituya una medida necesaria para la salvaguardia de:

a) la seguridad del Estado;

b) la defensa;

c) la seguridad pública;

d) la prevención, la investigación, la detección y la represión de infracciones penales o de las infracciones de la deontología en las profesiones reglamentadas;

e) un interés económico y financiero importante de un Estado miembro o de la Unión Europea, incluidos los asuntos monetarios, presupuestarios y fiscales;

f) una función de control, de inspección o reglamentaria relacionada, aunque solo sea ocasionalmente, con el ejercicio de la autoridad pública en los casos a que hacen referencia las letras c), d) y e);

g) la protección del interesado o de los derechos y libertades de otras personas.

[…]»

B. *Derecho nacional*

19. El artículo 12 de la Telemediengesetz (Ley de servicios de información y comunicación electrónica; en lo sucesivo, «TMG») [6] prescribe:

«1. El prestador de servicios solo podrá recoger y utilizar datos personales para prestar los servicios de telecomunicación en la medida en que lo permitan la presente ley u otras disposiciones referidas expresamente a dichos servicios, o el usuario haya prestado su consentimiento.

2. El prestador de servicios sólo podrá utilizar para otros fines los datos personales recogidos para prestar los servicios de telecomunicación en la medida en que lo permitan la presente ley u otras disposiciones referidas expresamente a dichos servicios, o el usuario haya prestado su consentimiento.

3. Salvo disposición en contrario, serán de aplicación las correspondientes disposiciones relativas a la protección de datos personales, aun cuando no se produzca un tratamiento automático de los datos.»

6 — Ley de 26 de febrero de 2007 (BGBl 2007 I, p. 179).

20. Con arreglo al artículo 15 de la TMG:

«1. El prestador de servicios sólo podrá recoger y utilizar los datos personales de un usuario cuando sea necesario para posibilitar el uso y la facturación de los servicios de telecomunicación (datos de uso). Se consideran datos de uso, en particular:

1. º los datos de identificación del usuario;

2. º los datos de comienzo y fin del uso y de su alcance, y

3. º los datos de los servicios de telecomunicación utilizados por el usuario.

2. El prestador de servicios podrá combinar los datos de uso de un usuario sobre la utilización de distintos servicios de telecomunicación siempre que sea necesario para fines de facturación frente al usuario.

[…]

4. El prestador de servicios podrá utilizar los datos de uso más allá de la conclusión de la operación de uso siempre que sea necesario para fines de facturación frente al usuario (datos de facturación). Para cumplir los plazos legales, estatutarios o contractuales de conservación vigentes, el prestador de servicios podrá bloquear los datos. [...]»

21. De conformidad con el artículo 3, apartado 1, de la Bundesdatenschutzgesetz (Ley federal de protección de datos; en lo sucesivo, «BDSG»),[7] «los datos personales son datos concretos sobre circunstancias personales o materiales de una persona física identificada o identificable (interesado). [...]».

II. Hechos

22. El Sr. Breyer ha instado contra la República Federal de Alemania una acción de cesación por el registro de direcciones IP.

23. Muchas instituciones públicas alemanas mantienen portales de Internet accesibles al público, en los que ofrecen información actualizada. Para prevenir ataques y posibilitar la persecución penal de los agresores, la mayor parte de esos portales almacenan todos los accesos en ficheros o registros de protocolo. En ellos conservan, incluso después de acabada la operación, el nombre del fichero o de la página solicitados, los conceptos introducidos en los campos de búsqueda, el momento de la llamada, la cantidad de datos transmitidos, la constatación del éxito de la llamada y la dirección IP del ordenador desde el que se ha hecho.

24. El Sr. Breyer, quien consultó varias de las páginas mencionadas, solicitó en su demanda que la República Federal fuera condenada a cesar en el registro, por sí misma o por terceros, de la dirección IP del sistema *host* desde el que realizó las llamadas, siempre que no fuera preciso para restablecer la disponibilidad del servicio de telecomunicación en caso de fallo.

7 — Ley de 20 de diciembre de 1990 (BGBl 1990 I, p. 2954).

25. La demanda del Sr. Breyer fue desestimada en primera instancia. Su recurso de apelación, sin embargo, fue estimado parcialmente, condenándose a la República Federal a cesar en el registro más allá del término de cada operación de acceso. La orden de cese se condicionó a que el demandante facilitara, durante la operación de acceso, sus datos personales, incluso en forma de dirección de correo electrónico, y a que el registro no fuera imprescindible para restablecer la disponibilidad del servicio de telecomunicación.

III. Cuestión planteada

26. Interpuesto recurso de casación por ambas partes, la Sala VI del Bundesgerichtshof (Tribunal Supremo Civil y Penal, Alemania) ha formulado las presentes cuestiones prejudiciales, remitidas el 17 de diciembre de 2014:

«1) ¿Debe interpretarse el artículo 2, letra a), de la Directiva 95/46/CE […] en el sentido de que una dirección de protocolo de Internet (dirección IP) almacenada por un prestador de servicios en relación con un acceso a su página web constituye para este un dato personal desde el momento en que un tercero (en este caso, un proveedor de acceso) disponga de los datos adicionales que permiten identificar al interesado?

2) ¿Se opone el artículo 7, letra f), de la Directiva de protección de datos a una disposición nacional con arreglo a la cual un prestador de servicios solo puede recoger y utilizar los datos personales de un usuario sin su consentimiento cuando sea necesario para ofrecer y facturar el uso concreto del servicio de telecomunicación por ese usuario, y con arreglo a la cual el objetivo de garantizar el funcionamiento del servicio de telecomunicación no puede justificar la utilización de esos datos tras la conclusión de cada operación de uso concreta?»

27. Según explica el tribunal de reenvío, el demandante podría exigir, conforme al derecho alemán, el cese del registro de las direcciones IP, si su conservación constituye una injerencia ilícita, de acuerdo con la legislación sobre protección de datos, en su derecho general a la personalidad, más específicamente, en su derecho a la «autodeterminación informativa» [artículos 1004, apartado 1, y 823, apartado 1, del Bürgerliches Gesetzbuch (Código Civil alemán), en relación con los artículos 1 y 2 de la Grundgesetz (Ley Fundamental)].

28. Así sería si: a) la dirección IP (en todo caso, junto con el momento de acceso a una página web) pudiera calificarse como «dato personal» en el sentido del artículo 2, letra a), en relación con el considerando 26, segunda frase, de la Directiva 95/46, o en el sentido del artículo 12, apartados 1 y 3, de la TMG, en relación el artículo 3, apartado 1, de la BDSG; y b) si no se cumpliera ningún supuesto de autorización en el sentido del artículo 7, letra f), de la Directiva 95/46 o en el sentido de los artículos 12, apartados 1 y 3, y 15, apartados 1 y 4, de la TMG.

29. Según el Bundesgerichtshof (Tribunal Supremo Civil y Penal), resulta ineludible, para interpretar el derecho nacional (artículo 12, apartado 1, de la TMG), saber cómo ha de entenderse el carácter personal de los datos a los que se refiere el artículo 2, letra a), de la Directiva 95/46.

30. Además, señala el tribunal *a quo*, como, según el artículo 15, apartado 1, de la TMG, el prestador de servicios solo podrá recoger y utilizar los datos personales de un usuario cuando sea indispensable para posibilitar la utilización y la facturación de los servicios de telecomunicación (datos de uso),[8] la interpretación de aquel precepto interno está ligada a la que se haga del artículo 7, letra f), de la Directiva 95/46.

8 — Según el Bundesgerichtshof (Tribunal Supremo Civil y Penal), los datos de uso son los identificativos del usuario, los del comienzo y el fin de la utilización y sobre su alcance, y los relativos a los servicios de telecomunicación que aquel ha empleado.

IV. El procedimiento ante el Tribunal de Justicia. Alegaciones de las partes

31. Han presentado observaciones escritas los Gobiernos alemán, austriaco y portugués, además de la Comisión. Solo esta institución, así como el Sr. Breyer, han comparecido en la vista pública celebrada el 25 de febrero de 2016, en la que declinó participar el Gobierno alemán.

A. *Alegaciones de las partes en relación con la primera pregunta*

32. Según el Sr. Breyer, son datos de carácter personal incluso aquellos cuya combinación es únicamente posible desde el punto de vista teórico, es decir, partiendo de la base de un peligro potencial abstracto, importando poco si en la práctica esa combinación se lleva en efecto a cabo. A su juicio, que un organismo pueda ser relativamente incapaz de identificar a una persona valiéndose de la dirección IP no significa que no exista un peligro para dicha persona. Por lo demás, en su opinión, es relevante el hecho de que Alemania conserva sus datos IP para, llegado el caso, identificar eventuales ataques o incoar acciones penales, según permite el artículo 113 de la Telekommunikationsgesetz (Ley sobre las telecomunicaciones) y ha ocurrido en numerosas ocasiones.

33. Para el Gobierno alemán, la primera pregunta merece una respuesta negativa. A su juicio, las direcciones IP dinámicas no revelan a una persona «identificada», en el sentido del artículo 2, letra a), de la Directiva 95/46. Para decidir si informan sobre una persona «identificable», en el sentido de ese mismo precepto, el examen de la *identificabilidad* debe realizarse con un criterio «relativo». Así se desprende, a su juicio, del considerando 26 de la Directiva 95/46, según el cual únicamente han de tenerse en cuenta los medios susceptibles de ser «razonablemente» utilizados por el responsable del tratamiento, o por un tercero, para la identificación de una persona. Tal puntualización indicaría que el legislador de la Unión no ha querido incluir en el ámbito de aplicación de la Directiva 95/46 aquellas situaciones en las que una identificación es objetivamente posible por parte de cualquier tercero.

34. Entiende también el Gobierno alemán que el concepto de «datos de carácter personal», en el sentido del artículo 2, letra a), de la Directiva 95/46, debe interpretarse a la luz de la finalidad de esta Directiva, esto es, garantizar el respeto de los derechos fundamentales. La necesidad de protección de las personas físicas podría verse de manera diferente en función de quién posea los datos y de si dispone, o no, de los medios para servirse de ellos a efectos de identificarlas.

35. Sostiene el Gobierno alemán que el Sr. Breyer no es identificable a partir de las direcciones IP combinadas con los otros datos que conservan los proveedores de contenidos. Para eso se habría de manejar la información que poseen los proveedores de acceso a Internet, quienes, en ausencia de base legal, no pueden facilitarla a los proveedores de contenidos.

36. Para el Gobierno austriaco, por el contrario, la respuesta debe ser afirmativa. De acuerdo con el considerando 26 de la Directiva 95/46, para que una persona sea tenida por identificable no se precisa que todos sus datos de identificación se encuentren en manos de una sola entidad. Así, una dirección IP podría ser un dato de carácter personal si un tercero (como, por ejemplo, el proveedor de acceso a Internet) dispone de los medios para identificar al titular de esa dirección, sin desplegar esfuerzos desmedidos.

37. El Gobierno portugués se inclina igualmente por una respuesta afirmativa, estimando que la dirección IP, en combinación con la fecha de la sesión de consulta, es un dato de carácter personal, en la medida en que puede conducir a la identificación del usuario por una entidad distinta de la que ha guardado la dirección IP.

38. La Comisión propone también una respuesta afirmativa, apoyándose en la solución adoptada por el Tribunal de Justicia en el asunto Scarlet Extended.[9] Para la Comisión, puesto que almacenar las direcciones IP sirve precisamente para identificar a los usuarios en caso de ataques cibernéticos, el empleo de los datos suplementarios que registran los proveedores de acceso a Internet supondría un medio que puede ser utilizado «razonablemente», en el sentido del considerando 26 de la Directiva 95/46. En definitiva, a juicio de la Comisión, tanto el objetivo perseguido por esta Directiva como los artículos 7 y 8 de la Carta de los derechos fundamentales de la Unión Europea (en lo sucesivo, «Carta») militarían en favor de una interpretación amplia del artículo 2, letra a), de la Directiva 95/46.

B. *Alegaciones de las partes en relación con la segunda pregunta*

39. Para el Sr. Breyer, el artículo 7, letra f), de la Directiva 95/46 constituye una cláusula general cuya puesta en práctica requiere concreción. De acuerdo con la jurisprudencia del Tribunal de Justicia, se trataría, por tanto, de valorar las circunstancias del caso particular y determinar si hay grupos con un interés legítimo, en el sentido de aquel precepto, siendo así que no solo está permitida, sino que es indispensable la previsión de reglas específicas para tales grupos, a los fines de aplicar ese artículo. En ese supuesto, y siempre para el Sr. Breyer, la normativa nacional sería compatible con el artículo 7, letra f), de la Directiva 95/46, por cuanto no existe un interés del portal público en la conservación de datos de carácter personal, o porque tiene mayor peso el interés en proteger el anonimato. Señala, sin embargo, que una conservación sistemática y con carácter personal de los datos no es conforme con una sociedad democrática, ni necesaria ni proporcionada para asegurar el funcionamiento de los medios electrónicos, perfectamente posible sin el registro de estos datos de carácter personal, como demostrarían los sitios web de algunos ministerios federales.

40. Cree el Gobierno alemán que no ha lugar a abordar la segunda pregunta, planteada únicamente en la hipótesis de que la primera mereciera una solución afirmativa, lo que, en su opinión, no es el caso, por los motivos antedichos.

41. El Gobierno austriaco propone responder que la Directiva 95/46 no es contraria, de manera general, a la conservación de datos como los controvertidos en el proceso principal, cuando sea imprescindible para garantizar el buen funcionamiento de los medios electrónicos. Para este Gobierno, una conservación limitada de la dirección IP, más allá de la duración de la consulta de una página web, puede ser lícita, por lo que respecta a la obligación del responsable del tratamiento de los datos de carácter personal de aplicar las medidas de protección de estos datos que impone el artículo 17, apartado 1, de la Directiva 95/46. La lucha contra los ataques cibernéticos puede legitimar el análisis de los datos relativos a ataques anteriores y que se deniegue el acceso a la página de Internet a algunas direcciones IP. La proporcionalidad de la conservación de datos como los implicados en el proceso principal, desde el punto de vista del objetivo de la garantía del buen funcionamiento de los medios electrónicos, debería apreciarse caso por caso, teniendo en cuenta los principios enunciados en el artículo 6, apartado 1, de la Directiva 95/46.

42. El Gobierno portugués defiende que el artículo 7, letra f), de la Directiva 95/46 no se opone a las normas nacionales implicadas en el proceso principal, porque el legislador alemán ya habría realizado la ponderación, prescrita en aquel precepto, entre los intereses legítimos del responsable del tratamiento de los datos de carácter personal, por un lado, y los derechos y libertades de los titulares de dichos datos, por otro.

9 — Sentencia de 24 de noviembre de 2011 (C-70/10, EU:C:2011:771), apartado 51.

43. Para la Comisión, la normativa nacional que incorpora el artículo 7, letra f), de la Directiva 95/46 ha de definir los objetivos del tratamiento de datos de carácter personal de manera que sean previsibles para el particular afectado. Destaca que la normativa alemana no respetaría esta exigencia al recoger, en el artículo 15, apartado 1, de la TMG, que la conservación de las direcciones IP se autoriza «cuando sea necesario para posibilitar el uso […] de los servicios de telecomunicación».

44. La Comisión sugiere, pues, como respuesta a la segunda pregunta, que este precepto se opone a la interpretación de una disposición nacional según la cual una autoridad pública que actúa como proveedor de servicios puede recopilar y utilizar los datos de carácter personal de un usuario sin su consentimiento, incluso aunque el objetivo que se persigue sea asegurar el buen funcionamiento general del medio electrónico, si la referida disposición nacional no establece ese objetivo de un modo suficientemente claro y preciso.

V. Apreciación

A. *Primera pregunta*

1. Delimitación de la cuestión planteada

45. De acuerdo con los términos en los que el Bundesgerichtshof (Tribunal Supremo Civil y Penal) la ha formulado, la primera de sus preguntas prejudiciales pretende dilucidar si una dirección IP, con la que se accede a una página web, representa para la entidad pública titular de esa página un dato personal [en el sentido del artículo 2, letra a), de la Directiva 95/46/CE], en el caso de que el proveedor de acceso a la red posea datos adicionales que permitan la identificación del interesado.

46. Así redactada, la pregunta es lo suficientemente precisa como para descartar, de entrada, otras que podrían suscitarse *in abstracto* sobre la naturaleza jurídica de las direcciones IP, en el contexto de la protección de datos de carácter personal.

47. En primer lugar, el Bundesgerichtshof (Tribunal Supremo Civil y Penal) se refiere exclusivamente a las «direcciones IP dinámicas», esto es, las que se asignan de forma temporal para cada conexión a la red y se modifican con ocasión de conexiones posteriores. Quedan, pues, al margen las «direcciones IP fijas o estáticas», caracterizadas por ser invariables y permitir la identificación permanente del dispositivo conectado a la red.

48. En segundo lugar, el tribunal de reenvío parte de la presunción de que el proveedor de la página web no está, en el proceso *a quo*, en condiciones de identificar, mediante la dirección IP dinámica, a quienes visitan sus páginas, ni cuenta por sí mismo con datos adicionales que, combinados con aquella dirección IP, faciliten su identificación. El Bundesgerichtshof (Tribunal Supremo Civil y Penal) parece entender que, en ese contexto, la dirección IP dinámica no sería un dato personal, en el sentido del artículo 2, letra a), de la Directiva 95/46, *para el proveedor de la página web*.

49. La duda del tribunal de reenvío tiene que ver con la posibilidad de que la dirección IP dinámica se califique, para el proveedor de la página web, como dato de carácter personal *si un tercero dispone de datos adicionales* que, combinados con ella, identifican a quienes consultan sus páginas. Ahora bien, y esta es una precisión más de interés, el Bundesgerichtshof (Tribunal Supremo Civil y Penal) no se refiere a cualquier tercero poseedor de los datos adicionales, sino solo al proveedor de acceso a la red (excluye, por tanto, a otros posibles poseedores de ese género de datos).

50. Quedan así fuera de debate, entre otros aspectos, los siguientes: a) si las direcciones IP estáticas son datos de carácter personal conforme a la Directiva 95/46;[10] b) si las direcciones IP dinámicas son, siempre y bajo cualquier circunstancia, datos de carácter personal en el sentido de esa Directiva; y, en fin, c) si la calificación de las direcciones IP dinámicas como datos de carácter personal es inevitable tan pronto como exista un tercero, cualquiera que sea, capaz de utilizarlas para la identificación de los usuarios de la red.

51. Se trata, pues, únicamente, de decidir si una dirección IP dinámica es un dato de carácter personal para el proveedor de un servicio de Internet cuando la compañía de comunicaciones que ofrece el acceso a la red (el proveedor de acceso) maneja datos adicionales que, combinados con aquella dirección, permiten identificar a quien accede a la página web gestionada por el primero.

2. Sobre el fondo

52. La cuestión que suscita este reenvío está siendo objeto en la doctrina y en la jurisprudencia alemanas de un intenso debate, polarizado en dos corrientes de opinión.[11] Según una (la que opta por un criterio «objetivo» o «absoluto»), un usuario resulta identificable –y, por lo tanto, la dirección IP es un dato personal susceptible de protección– cuando, cualesquiera que sean las aptitudes y los medios del proveedor del servicio de Internet, su identificación es factible con solo combinar esa dirección IP dinámica con los datos aportados por un tercero (por ejemplo, el proveedor de acceso a la red).

53. Para los partidarios de la otra corriente (los que defienden un criterio «relativo»), la posibilidad de contar con la ayuda de un tercero, en la identificación final del usuario, no basta para atribuir carácter personal a la dirección IP dinámica. Lo relevante es la capacidad de quien tiene acceso al dato para servirse de él, con sus propios medios, e identificar así a una persona.

54. Cualesquiera que sean los términos de esa controversia en el derecho interno, la respuesta del Tribunal de Justicia debe limitarse a interpretar las dos previsiones de la Directiva 95/46, a las que han aludido tanto el tribunal *a quo* como las partes del proceso, esto es, su artículo 2, letra a),[12] y su considerando 26.[13]

55. Las direcciones IP dinámicas, solo por facilitar información sobre la fecha y la hora en las que se ha accedido a una página web desde un ordenador (u otro dispositivo), manifiestan unas ciertas pautas del comportamiento de los usuarios de Internet y, por lo tanto, suponen una potencial injerencia en el derecho a la vida privada,[14] garantizado por el artículo 8 del Convenio Europeo para la Protección de

10 — Problema zanjado por el Tribunal de Justicia en las sentencias de 24 de noviembre de 2011 Scarlet Extended (C-70/10, EU:C:2011:771), apartado 51; y de 19 de abril de 2012, Bonnier Audio y otros (C-461/10, EU:C:2012:219). En los apartados 51 y 52 de esta última sentencia, el Tribunal de Justicia concluyó que la comunicación, «a efectos de su identificación, [d]el nombre y la dirección […] de un usuario de Internet que hace uso de la dirección IP a partir de la cual presuntamente se intercambiaron de forma ilícita archivos que contenían obras protegidas […] constituye un tratamiento de datos de carácter personal en el sentido del artículo 2, párrafo primero, de la Directiva 2002/58, en relación con el artículo 2, letra b), de la Directiva 95/46».

11 — Sobre ambas posiciones doctrinales, pueden verse, por ejemplo, Schreibauer, M., en *Kommentar zum Bundesdatenschutzgesetz. Nebengesetze*, Esser, M., Kramer, P., y von Lewinski, K. (eds.), Carl Heymanns Verlag/Wolters Kluwer, Colonia, 2014, 4.ª ed., § 11 Telemediengesetz (4 a 10); Nink, J., y Pohle, J.: «Die Bestimmbarkeit des Personenbezugs. Von der IP-Adresse zum Anwendungsbereich der Datenschutzgesetze», en *Multimedia und Recht*, 9/2015, pp. 563 a 567; Heidrich, J., y Wegener, C.: «Rechtliche und technische Anforderungen an die Protokollierung von IT-Daten. Problemfall Logging», en *Multimedia und Recht*, 8/2015, pp. 487 a 492; Leisterer, H.: «Die neuen Pflichten zur Netz– und Informationssicherheit und die Verarbeitung personenbezogener Daten zur Gefahrenabwehr», en *Computer und Recht*, 10/2015, pp. 665 a 670.

12 — Transcrito en el punto 13.

13 — Transcrito en el punto 11.

14 — Así lo recordó el abogado general Cruz Villalón en las conclusiones presentadas en el asunto Scarlet Extended (C-70/10, EU:C:2011:255), punto 76, y así lo entiende el Supervisor Europeo de Protección de Datos en sus dictámenes de 22 de febrero de 2010, sobre las negociaciones que mantiene la Unión Europea sobre un Acuerdo Comercial de Lucha contra la Falsificación (ACTA) (DO, 2010, C 147, p. 1, apartado 24), y de 10 de mayo de 2010, sobre la propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la lucha contra los abusos sexuales, la explotación sexual de los niños y la pornografía infantil, por la que se deroga la Decisión marco 2004/68/JAI (DO 2010, C 323, p. 6, apartado 11).

los Derechos Humanos y de las Libertades Fundamentales y por el artículo 7 de la Carta, a cuya luz, así como a la del artículo 8 de la misma, debe interpretarse la Directiva 95/46.[15] En realidad, las partes del litigo no ponen en duda esta premisa, que tampoco es objeto, en cuanto tal, de la pregunta perjudicial.

56. La persona a la que dichos pormenores atañen no es una «persona física identificada». La fecha y la hora de una conexión, así como su origen numérico, no revelan, directa ni inmediatamente, quién es la persona física a la que pertenece el dispositivo desde el que se visita la página web, tampoco la identidad del usuario que lo maneja (puede ser cualquier persona física).

57. Sin embargo, en la medida en que una dirección IP dinámica ayuda a determinar —bien por sí sola, bien en unión de otros datos— quién es el titular del dispositivo utilizado para el acceso a la página web, puede calificarse de una información sobre una «persona identificable».[16]

58. Según el planteamiento del Bundesgerichtshof (Tribunal Supremo Civil y Penal), la dirección IP dinámica no es suficiente, por sí sola, para identificar al usuario que a través de ella ha accedido a una página web. Si el proveedor del servicio de Internet pudiese, por el contrario, a través de la dirección IP dinámica, identificar al usuario, se trataría, sin ninguna duda, de un dato de carácter personal con arreglo a la Directiva 95/46. No parece, sin embargo, que este sea el sentido de la pregunta prejudicial, en la que subyace que los proveedores de servicios de Internet implicados en el litigio *a quo* no pueden identificar al usuario a partir, exclusivamente, de la dirección IP dinámica.

59. Combinada con otros datos, la dirección IP dinámica facilita la identificación «indirecta» del usuario, idea en la que todos coinciden. La eventualidad de que existan esos datos adicionales, asociables con la dirección IP dinámica, ¿autoriza, sin más, a catalogar esta última como un dato de carácter personal a tenor de la Directiva? Habrá que resolver si basta, a tales efectos, la mera posibilidad, en abstracto, de conocer esos datos o si, por el contrario, es preciso que estén disponibles para quien ya sabe la dirección IP dinámica, o para un tercero.

60. Las partes han centrado sus observaciones en la interpretación del considerando 26 de la Directiva 95/46, de cuyo contenido destacan la expresión «medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona». La pregunta del tribunal de reenvío no se refiere a datos adicionales, en poder de los proveedores de servicio implicados en el proceso principal. Tampoco alude a cualquier tercero, poseedor de esos datos adicionales (cuyo cruce con la dirección IP dinámica facilite la identificación del usuario), sino al proveedor de acceso a la red.

61. No es necesario, pues, que en este caso el Tribunal de Justicia analice todos los medios que podría utilizar «razonablemente» la parte demandada en el proceso *a quo* para que las direcciones IP dinámicas con las que cuenta puedan calificarse de datos de carácter personal. Como el Bundesgerichtshof (Tribunal Supremo Civil y Penal) se refiere únicamente a datos adicionales en

15 — Véanse, en este sentido, la sentencia de 20 de mayo de 2003, Österreichischer Rundfunk (C-465/00, C-138/01 y C-139/01, EU:C:2003:294), apartado 68; y las conclusiones de la abogado general Kokott presentadas en el asunto Promusicae (C-275/06, EU:C:2007:454), puntos 51 y ss.

16 — Cabe presumir que, salvo prueba en contrario, dicha persona es la que ha navegado por Internet y accedido a la página web correspondiente. Con todo, aun prescindiendo de esta última presunción, la información acerca de la fecha, la hora y el origen numérico del acceso a una página web permitiría vincular ese acceso con el titular del dispositivo y asociarlo indirectamente a las pautas de su comportamiento en la red. La excepción imaginable serían las direcciones IP asignadas a ordenadores de locales como los *ciber cafés*, cuyos usuarios anónimos resultan inidentificables y sobre cuyos propietarios el tráfico generado en el local no brinda ninguna información personal relevante. Esta es, por lo demás, la única excepción al principio de que las direcciones IP son datos personales admitida por el Grupo de protección de las personas en lo que respecta al tratamiento de datos personales, creado por la Directiva 95/46 (el denominado «Grupo del artículo 29»). Puede leerse su Dictamen 4/2007, de 20 de junio de 2007, sobre el concepto de datos de carácter personal, WP 136, en http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.

manos de un tercero, puede inferirse: a) bien que la demandada no tiene datos adicionales propios para que permitan la identificación del usuario; o b) bien que, si tiene a su alcance esos datos, no está en condiciones de utilizarlos razonablemente con ese propósito, en cuanto responsable de su tratamiento, según el considerando 26 de la Directiva 95/46.

62. Ambas hipótesis dependen de una constatación de carácter fáctico que solo compete a la jurisdicción de reenvío. El Tribunal de Justicia podría facilitarle criterios de orden general para interpretar los términos «medios que puedan ser razonablemente utilizados por el responsable del tratamiento», si el Bundesgerichtshof (Tribunal Supremo Civil y Penal) tuviera alguna duda sobre la capacidad de la demandada para servirse razonablemente de datos adicionales propios. No siendo así, está fuera de lugar, a mi juicio, que el Tribunal de Justicia marque ahora unos criterios de interpretación que no son imprescindibles para el tribunal de reenvío, ni los ha solicitado.

63. El núcleo de la cuestión planteada se contrae, por lo tanto, a resolver si es relevante, para calificar las direcciones IP dinámicas de datos personales, la circunstancia de que un tercero muy específico —el proveedor de acceso a Internet— disponga de datos adicionales que, combinados con esas direcciones, tienen aptitud para identificar al usuario que ha visitado una determinada página web.

64. De nuevo se impone la mención al considerando 26 de la Directiva 95/46. Los términos «medios que puedan ser razonablemente utilizados […] *por cualquier otra persona*» [17] podrían dar pie a una interpretación según la cual bastaría que algún tercero pudiera conseguir datos adicionales (susceptibles de ser combinados con una dirección IP dinámica a fin de identificar a una persona), para pensar que esa dirección constituye *eo ipso* un dato de carácter personal.

65. Esa interpretación maximalista llevaría, en la práctica, a clasificar como dato personal todo tipo de información, por más insuficiente que sea en sí misma para facilitar la identificación de un usuario. Nunca podrá descartarse, con absoluta certeza, que no haya un tercero en posesión de datos adicionales susceptibles de ser combinados con aquella información y aptos, en consecuencia, para desvelar la identidad de una persona.

66. En mi opinión, la posibilidad de que el avance de los medios técnicos allane sensiblemente, en un futuro más o menos inmediato, el camino del acceso a instrumentos de obtención y tratamiento de información, cada vez más sofisticados, justifica las cautelas con las que se quiere anticipar la defensa de la intimidad. Se ha procurado que, al definir las categorías jurídicas relevantes en el ámbito de la protección de los datos, se incluyan hipótesis de comportamiento suficientemente amplias y flexibles para ofrecer la cobertura a cualquier supuesto imaginable. [18]

67. Creo, sin embargo, que esa preocupación —por lo demás muy legítima— no puede llevar a ignorar los términos de la voluntad normativa del legislador y que la interpretación sistemática del considerando 26 de la Directiva 95/46 se contrae a «los medios que puedan ser razonablemente utilizados» *por ciertos terceros*.

68. Al igual que el considerando 26 no alude a cualesquiera medios utilizables por el responsable del tratamiento (en este caso, el prestador de servicios de Internet), sino solo a los que este pueda utilizar «razonablemente», así también ha de entenderse que el legislador se refiere a los «terceros» a los que, *también de manera razonable*, puede acudir el responsable del tratamiento que pretenda obtener los datos adicionales para la identificación. No ocurrirá así cuando el contacto con esos terceros sea, de hecho, muy costoso en términos humanos y económicos, o prácticamente irrealizable o prohibido por

17 — Sin cursiva en el original.

18 — Esa vocación cautelar y preventiva está en la base de la postura mantenida por el Grupo del artículo 29, para quien, como he señalado, debe partirse del principio de que las direcciones IP constituyen un dato de carácter personal, admitiendo como única excepción la hipótesis de que el prestador del servicio esté en posición de determinar con absoluta certeza que son direcciones que corresponden a personas inidentificables, como pueden ser los usuarios de un *ciber café*. Véase la nota 16, *in fine*.

la ley. De otra forma, como antes advertía, sería prácticamente imposible discriminar entre unos medios y otros, pues siempre cabría imaginar la contingencia de un tercero que, por inaccesible que resulte al prestador de servicios de Internet, pueda contar —ahora, o en el futuro— con datos adicionales pertinentes para coadyuvar a la identificación de un usuario.

69. Según he adelantado, el tercero al que alude el Bundesgerichtshof (Tribunal Supremo Civil y Penal) es un proveedor de acceso a la red. Es, seguramente, el tercero al que resulta más razonable pensar que se dirija el prestador de servicios para recabar los datos adicionales precisos, si pretende identificar de la manera más eficaz, práctica y directa al usuario que ha accedido a su página web gracias a la dirección IP dinámica. No es, en modo alguno, un tercero hipotético, desconocido e inaccesible, sino un protagonista principal en el entramado de Internet, de quien se sabe con certeza que está en posesión de los datos que requiere el prestador de servicios para identificar a un usuario. De hecho, tal y como relata el tribunal de reenvío, es a ese concreto tercero a quien tiene intención de dirigirse la demandada en el proceso principal para recabar los datos adicionales que le son imprescindibles.

70. El proveedor de acceso a Internet es, típicamente, el tercero al que apunta el considerando 26 de la Directiva 95/46, a quien de manera más «razonable» puede acudir el prestador de servicios del proceso *a quo*. Queda por dilucidar, sin embargo, si la obtención de los datos adicionales en poder de ese tercero puede calificarse de «razonablemente» viable o practicable.

71. El Gobierno alemán sostiene que, siendo la información que obra en poder del proveedor de acceso a Internet un dato de carácter personal, aquel no puede facilitarlo sin más, sino de acuerdo con la normativa reguladora del tratamiento de estos datos. [19]

72. Sin duda así es, pues para disfrutar de esa información ha de estarse a la legislación aplicable a los datos de carácter personal. Una información solo puede obtenerse «razonablemente» si se cumplen las condiciones que rigen el acceso a ese género de datos, la primera de las cuales es la posibilidad legal de su conservación y transmisión a otros. Es cierto que el proveedor de acceso a Internet está facultado para rechazar la entrega de los datos interesados, pero cabe también lo contrario. La posibilidad de transmisión de datos, perfectamente «razonable», convierte por sí sola a la dirección IP dinámica, conforme a los términos del considerando 26 de la Directiva 95/46, en un dato de carácter personal para el prestador de servicios de Internet.

73. Se trata de una eventualidad factible *en el marco de la ley* y, por eso, «razonable». Los medios de acceso razonables que menciona la Directiva 95/46 han de ser, por definición, medios lícitos. [20] Tal es la premisa de la que, como es natural, parte el tribunal de reenvío, según recuerda el Gobierno alemán. [21] Así se reducen de modo significativo las vías de acceso jurídicamente relevantes, pues habrán de ser, en exclusiva, las de carácter lícito. Pero mientras estas existan, por restrictivas que puedan ser en su aplicación práctica, suponen un «medio razonable», en el sentido de la Directiva 95/46.

74. En consecuencia, opino que, en los términos planteados por el Bundesgerichtshof (Tribunal Supremo Civil y Penal), la primera de sus preguntas merece una respuesta afirmativa. La dirección IP dinámica debe ser catalogada, para el proveedor de servicios de Internet, como un dato de carácter personal habida cuenta de la existencia de un tercero (el proveedor de acceso a la red) al que puede razonablemente dirigirse para conseguir otros datos adicionales que, entrecruzados con aquella, propicien la identificación de un usuario.

19 — Apartados 40 y 45 de sus observaciones escritas.

20 — Es irrelevante, en este contexto, que el acceso al dato personal sea posible *de facto* mediando la infracción de las leyes de protección de datos.

21 — Apartados 47 y 48 de sus observaciones escritas.

75. El resultado al que conduciría la solución contraria a la que propugno creo que la refuerza. Si las direcciones IP dinámicas no constituyeran un dato de carácter personal para el prestador de servicios en Internet, este podría conservarlas de manera indefinida, y podría solicitar en cualquier momento al proveedor de acceso a Internet los datos adicionales para combinarlos con aquella e identificar al usuario. En estas circunstancias, tal y como admite el Gobierno alemán,[22] la dirección IP dinámica se convertiría en un dato de carácter personal, toda vez que ya tendría los datos adicionales válidos para identificar al usuario, aplicándose al respecto la legislación sobre protección de datos.

76. Ahora bien, se trataría de un dato cuya conservación sólo habrá sido posible por cuanto no se habría entendido, hasta entonces, como de carácter personal para el prestador de servicios. Quedaría así en manos de este último la calificación jurídica de la dirección IP dinámica como dato de carácter personal, condicionada a la eventualidad de que, en un momento futuro, decida utilizarla para identificar al usuario mediante su combinación con los datos adicionales que deberá recabar de un tercero. A mi juicio, sin embargo, lo determinante, a tenor de la Directiva 95/46, es la posibilidad —razonable— de la existencia de un tercero «accesible», que posea los medios necesarios para propiciar la identificación de una persona, no que la posibilidad de recurrir a ese tercero se materialice.

77. Podría admitirse incluso, con el Gobierno alemán, que la dirección IP dinámica únicamente se convierte en un dato de carácter personal tan pronto la recibe el prestador de acceso a Internet. Con todo, debería aceptarse entonces que esa calificación se habrá operado con efecto retroactivo, en cuanto al plazo de conservación de la dirección IP, y, en consecuencia, tenerla por inexistente, si se ha superado el tiempo durante el que podía conservarse de haber sido calificada desde un principio de dato de carácter personal. En esta tesitura se propiciaría un resultado contrario al espíritu de la legislación sobre protección de datos personales. La razón que justifica la conservación solo temporal de estos datos se vería defraudada ante la eventual demora de la relevancia de una cualidad que les es inherente desde el inicio: su virtualidad como medio de identificación —por sí, o en unión de otros datos— de una persona física. También por esta razón, de pura economía, es más razonable atribuirle ese carácter desde el comienzo.

78. Por tanto, como primera conclusión, entiendo que el artículo 2, letra a), de la Directiva 95/46 debe interpretarse en el sentido de que una dirección IP almacenada por un prestador de servicios en relación con un acceso a su página web constituye para este un dato personal, en la medida en que un proveedor de acceso a la red (Internet) disponga de los datos adicionales que permitan identificar al interesado.

B. *Segunda pregunta*

79. Con la segunda de sus preguntas prejudiciales el Bundesgerichtshof (Tribunal Supremo Civil y Penal) quiere saber si el artículo 7, letra f), de la Directiva 95/46 se opone a una normativa nacional que solo acepta la recogida y la utilización de los datos personales de un usuario, sin su consentimiento, cuando sea necesario para ofrecer y facturar el uso concreto del servicio de telecomunicación por ese usuario, sin que el objetivo de garantizar el funcionamiento del servicio pueda justificar la utilización de esos datos una vez terminada cada operación de uso.

80. La respuesta debe ir precedida de una puntualización sobre la información facilitada por el Bundesgerichtshof (Tribunal Supremo Civil y Penal), según la cual los datos litigiosos se conservan para asegurar el buen funcionamiento de los sitios Internet implicados en el proceso principal, posibilitando, en su caso, la persecución penal de los ataques cibernéticos de que pudieran ser objeto.

22 — Apartado 36 de sus observaciones escritas.

81. Hay que plantearse, pues, ante todo, si el tratamiento de las direcciones IP a las que alude el reenvío está comprendido en la excepción prevista en el artículo 3, apartado 2, primer guion, de la Directiva 95/46.[23]

1. Sobre la aplicabilidad de la Directiva 95/46 al tratamiento de los datos litigiosos

82. La República Federal de Alemania actúa en el proceso principal, según parece, como mero prestador de servicios de Internet, es decir, como un particular (y, por lo tanto, *sine imperio*). De este hecho se deduce que, en principio, el tratamiento de los datos objeto de este litigio no está excluido del ámbito de aplicación de la Directiva 95/46.

83. En palabras del Tribunal de Justicia en la sentencia Lindqvist,[24] las actividades del artículo 3, apartado 2, de la Directiva 95/46 «son, en todos los casos, actividades propias del Estado o de las autoridades estatales y ajenas a la esfera de actividades de los particulares».[25] En la medida en que el tratamiento de los datos debatidos tenga como responsable a quien, pese a su condición de autoridad pública, actúa en realidad como un sujeto privado, es aplicable la Directiva 95/46.

84. El tribunal de reenvío, al destacar la finalidad principal que la Administración alemana persigue con el registro de las direcciones IP dinámicas, subraya que pretende «garantizar y mantener la seguridad y el funcionamiento de sus servicios de telecomunicación»; en especial, promover «la detección y la defensa frente a los frecuentes ataques "denial of service", en que la infraestructura de telecomunicaciones queda paralizada por una avalancha deliberada y coordinada por determinados servidores de red de una cantidad ingente de solicitudes».[26] La conservación de las direcciones IP dinámicas con este propósito es común a cualquier titular de sitios web de una cierta importancia y no implica, ni directa ni indirectamente, el ejercicio de poder público, por lo que su inclusión en el ámbito de la Directiva 95/46 no entraña una dificultad excesiva.

85. El Bundesgerichtshof (Tribunal Supremo Civil y Penal) asevera, sin embargo, que la conservación de las direcciones IP dinámicas por los prestadores de servicios implicados en el proceso principal responde también al designio de actuar penalmente, llegado el momento, contra los autores de eventuales ataques cibernéticos. ¿Basta este designio para excluir el tratamiento de esos datos del ámbito de aplicación de la Directiva 95/46?

86. En mi opinión, si por «actuación penal» se entiende el ejercicio del *ius puniendi* del Estado por los prestadores de servicio demandados en el proceso principal, nos encontraríamos ante una «actividad del Estado en materia penal» y, por tanto, ante una de las excepciones previstas en el artículo 3, apartado 2, primer guion, de la Directiva 95/46.

87. En esas circunstancias, con arreglo a la doctrina establecida por el Tribunal de Justicia en el asunto Huber,[27] el tratamiento de datos personales por los prestadores de servicio, en aras de la seguridad y del funcionamiento técnico de sus servicios de telecomunicación, estaría comprendido en el ámbito de aplicación de la Directiva 95/46, mientras que el tratamiento de datos dirigido a la actividad del Estado en materia penal permanecería al margen.

23 — No entra en el ámbito de aplicación de la Directiva 95/46 «el tratamiento de datos que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado […] y *las actividades del Estado en materia penal*» (sin cursiva en el original).

24 — Sentencia de 6 de noviembre de 2003 (C-101/01, EU:C:2003:596), apartado 43.

25 — En los mismos términos, la sentencia de 16 de diciembre de 2008, Satakunnan Markkinapörssi y Satamedia (C-73/07, EU:C:2008:727), apartado 41.

26 — Apartado 36 del auto de planteamiento de la cuestión prejudicial.

27 — Sentencia de 16 de diciembre de 2008 (C-524/06, EU:C:2008:724), apartado 45.

88. Del mismo modo, aun cuando la actuación penal propiamente dicha no correspondiera a la República Federal de Alemania, en tanto que mero prestador de servicios desprovisto de imperio, sino, como cualquier particular, se limitara a transferir las direcciones IP litigiosas a un órgano estatal para el ejercicio de una acción represiva, el tratamiento de las direcciones IP dinámicas tendría igualmente por objeto una actividad excluida del ámbito de la Directiva 95/46.

89. Así resulta de la jurisprudencia sentada en el asunto Parlamento/Consejo y Comisión,[28] en la que el Tribunal de Justicia afirmó que el hecho de que determinados datos personales «sean recogidos por operadores privados con fines mercantiles y de que sean estos quienes organizan su transferencia a un Estado tercero» no supone que esa transferencia «no esté incluida en el ámbito de aplicación» del artículo 3, apartado 2, primer guion, de la Directiva 95/46 cuando la finalidad de la transferencia tiene por objeto las actividades del Estado en materia penal, toda vez que en ese caso «se inserta en un marco creado por los poderes públicos y cuyo objetivo es proteger la seguridad pública».[29]

90. Por el contrario, si, como pienso, por «actuación penal» ha de entenderse, según se deduce del auto de reenvío, la que es propia de un particular en tanto que sujeto legitimado para instar la actuación del *ius puniendi* del Estado, mediante la correspondiente acción, entonces no cabe sostener que el tratamiento de las direcciones IP dinámicas tenga por objeto la actividad del Estado en materia penal, excluida del ámbito de aplicación de la Directiva 95/46.

91. En efecto, la conservación y el registro de ese dato servirían como un medio más de prueba con el que el titular de la página web puede solicitar del Estado la represión, a instancia de parte, de una conducta ilícita. Sería, en definitiva, un instrumento para la defensa, en vía penal, de los derechos reconocidos por el ordenamiento a un sujeto particular (en este caso, a una entidad pública que actúa en régimen de derecho privado). No se diferencia, desde esta óptica, de la iniciativa de cualquier otro proveedor de servicio de Internet que pretende la tutela del Estado con arreglo a los procedimientos de ejercicio de la acción penal establecidos por el ordenamiento.

92. En consecuencia, en la medida en que la Administración alemana se comporte como prestador de servicios de Internet desprovisto de poder público, lo que corresponde apreciar al tribunal de reenvío, el tratamiento que haga de las direcciones IP dinámicas, como datos de carácter personal, está comprendido en el ámbito de aplicación de la Directiva 95/46.

2. Sobre el fondo

93. El artículo 15, apartado 1, de la TMG solo autoriza la recogida y la utilización de los datos personales de un usuario cuando sea imprescindible para ofrecer y facturar un uso concreto del servicio de telecomunicación. Más exactamente, el prestador de servicios solo puede recoger y utilizar los denominados «datos de uso», esto es, los datos personales de un usuario indispensables para posibilitar «el uso y la facturación de los servicios de telecomunicación». Esos datos se deben eliminar en cuanto acabe la operación (esto es, en cuanto cese el uso concreto del servicio de telecomunicación), salvo que se hayan de guardar «para fines de facturación», según dispone el apartado 4 del mismo artículo 15 de la TMG.

28 — Sentencia de 30 de mayo de 2006 (C-317/04 y C-318/04, EU:C:2006:346), apartados 54 a 59.

29 — *Ibidem*, apartado 59. Versaba sobre datos personales cuyo tratamiento no era necesario para la prestación de servicios que constituía el negocio de los operadores privados afectados (compañías aéreas), pero que estos se veían obligados a transferir a las autoridades estadounidenses para prevenir y luchar contra el terrorismo.

94. Culminada la conexión, el artículo 15 de la TMG parece descartar que los datos de uso se almacenen por otros motivos; tampoco para garantizar «el uso de los servicios de telecomunicación» con carácter general. Al referirse exclusivamente a los fines de facturación como causa justificativa de la conservación de los datos, aquel precepto de la TMG podría leerse (aunque su interpretación definitiva corresponde a la jurisdicción de reenvío) como si reclamara que los datos de uso únicamente se empleen para posibilitar una relación concreta, y se supriman cuando concluya.

95. El artículo 7, letra f), de la Directiva 95/46 [30] legitima el tratamiento de datos personales en unos términos que calificaría de más generosos (para el responsable del tratamiento) que los previstos en el tenor literal del artículo 15 de la TMG. La norma alemana se puede tildar, en este extremo, de más restrictiva que la de la Unión, pues no contemplaría, en principio, la satisfacción de otro interés legítimo que no sea el vinculado a la facturación del servicio, siendo así que, en tanto que prestador de servicios en Internet, la República Federal de Alemania podría tener también un interés legítimo en asegurar el buen funcionamiento de sus páginas web, más allá de cada relación de uso. [31]

96. La doctrina del Tribunal de Justicia en la sentencia ASNEF y FECEMD [32] proporciona las pautas para responder a la segunda pregunta prejudicial. Afirmó entonces el Tribunal de Justicia que del objetivo perseguido por la Directiva 95/46 «se deduce […] que el artículo 7 de la Directiva 95/46 establece una lista exhaustiva y taxativa de los casos en que un tratamiento de datos personales puede considerarse lícito». [33] De ahí que «los Estados miembros no pueden ni añadir al artículo 7 de la Directiva 95/46 nuevos principios relativos a la legitimación de los tratamientos de datos personales ni imponer exigencias adicionales que vendrían a modificar el alcance de alguno de los seis principios establecidos en dicho artículo». [34]

97. El artículo 15 de la TMG no añade un requisito adicional a los previstos en el artículo 7 de la Directiva 95/46 para la licitud del tratamiento de datos —como sucedía en los asuntos ASNEF y FECEMD—, [35] pero, si se interpreta en el sentido restrictivo al que alude el tribunal *a quo*, reduce el contenido de la condición contemplada en la letra f) de dicho precepto: allí donde el legislador de la Unión se refiere, con carácter general, a la satisfacción del «[…] interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos», el artículo 15 de la TMG únicamente atendería a la necesidad de «posibilitar el uso [concreto] y la facturación de los servicios de telecomunicación».

98. Al igual que ocurría en los asuntos ASNEF y FECEMD, [36] también en este una medida nacional —de nuevo, si se interpretase en el sentido restrictivo antes explicado— modificaría el alcance de un principio del artículo 7 de la Directiva 95/46, más que circunscribirse a acotarlo, que es lo único para lo que las autoridades de cada Estado miembro poseen un cierto margen de apreciación, con arreglo al artículo 5 de la Directiva 95/46.

30 — Transcrito en el punto 17.

31 — Véase el punto 84. Ciertamente, los titulares de las páginas web ostentan un interés legítimo en prevenir y combatir las denegaciones de servicio («denials of service») que menciona el tribunal de reenvío, esto es, los ataques masivos que, en ocasiones, se lanzan, de modo concertado, contra algunos sitios web para saturarlos y dejarlos inoperantes.

32 — Sentencia de 24 de noviembre de 2011 (C-468/10 y C-469/10, EU:C:2011:777).

33 — *Ibidem*, apartado 30.

34 — *Ibidem*, apartado 32.

35 — Supuesto en el que la legislación nacional añadía a las exigencias del artículo 7, letra f), de la Directiva 95/46 la de que los datos objeto de tratamiento figuraran en fuentes accesibles al público.

36 — Sentencia de 24 de noviembre de 2011 (C-468/10 y C-469/10, EU:C:2011:777).

99. En efecto, según este último precepto, «los Estados miembros precisarán, dentro de los límites de las disposiciones del presente capítulo, [37] las condiciones en que son lícitos los tratamientos de datos personales». Sin embargo, tal y como se afirmó en los asuntos ASNEF y FECEMD, [38] «los Estados miembros tampoco pueden introducir, al amparo de lo dispuesto [en dicho precepto], principios relativos a la legitimación de los tratamientos de datos personales distintos a los enunciados en el artículo 7 de esa Directiva ni modificar, mediante exigencias adicionales, el alcance de los seis principios establecidos en dicho artículo 7».

100. El artículo 15 de la TMG reduciría sustancialmente, en relación al artículo 7, letra f), de la Directiva 95/46, el perímetro del interés legítimo relevante para justificar el tratamiento de datos, sin constreñirse a puntualizarlo o a matizarlo en los márgenes de lo autorizado por el artículo 5 de la misma Directiva. Lo haría, además, de forma rotunda y absoluta, sin consentir que la protección y la garantía del uso general del servicio de telecomunicación puedan ser objeto de ponderación con «el interés o los derechos y libertades fundamentales del interesado que requiera protección con arreglo al apartado 1 del artículo 1» de la Directiva 95/46, según prescribe el artículo 7, letra f), de esta última.

101. En definitiva, al igual que en los asuntos ASNEF y FECEMD, [39] el legislador estatal alemán habría prescrito «con carácter definitivo el resultado de la ponderación de los derechos e intereses en conflicto respecto de [determinadas categorías de datos personales], sin permitir un resultado diferente en atención a las circunstancias particulares de cada caso concreto», de manera que «no se trata ya de una precisión en el sentido del […] artículo 5» de la Directiva 95/46.

102. En estas circunstancias, opino que el Bundesgerichtshof (Tribunal Supremo Civil y Penal) está obligado a interpretar la legislación nacional de manera conforme con la Directiva 95/46, lo que implica: a) que se pueda incluir entre las causas justificativas del tratamiento de los denominados «datos de uso» el interés legítimo del prestador de servicios de telecomunicación para proteger el uso general de estos; y b) que se pueda ponderar, *ad casum*, ese interés del prestador del servicio, contrastándolo con el interés o los derechos y libertades fundamentales del usuario, para dilucidar el que haya de merecer protección según el artículo 1, apartado 1, de la Directiva 95/46. [40]

103. Nada más procede, a mi juicio, añadir sobre los términos en los que esta ponderación haya de realizarse en el caso que da origen al reenvío prejudicial. Nada pregunta sobre ese particular el Bundesgerichtshof (Tribunal Supremo Civil y Penal), preocupado por la solución de una cuestión previa a ese juicio de ponderación; a saber, si dicho juicio puede llevarse a cabo.

104. En fin, parece superfluo señalar que el tribunal *a quo* podrá tener en cuenta las eventuales disposiciones legales adoptadas por el Estado miembro en el marco de la autorización contenida en el artículo 13, apartado 1, letra d), de la Directiva 95/46, para recortar el alcance de las obligaciones y los derechos previstos en el artículo 6 de la misma Directiva, cuando fuese necesario para salvaguardar, entre otros bienes, «[…] la prevención, la investigación, la detección y la represión de infracciones penales […]». Tampoco a este extremo se refiere el tribunal de reenvío, consciente sin duda de la existencia de ambos artículos.

37 — Capítulo II, titulado «Condiciones generales para la licitud del tratamiento de datos personales», que comprende los artículos 5 a 21 de la Directiva 95/46.

38 — Sentencia de 24 de noviembre de 2011 (C-468/10 y C-469/10, EU:C:2011:777), apartado 36.

39 — *Ibidem*, apartado 47.

40 — En el acto de la vista, la defensa del Sr. Breyer rechazó que el registro de las direcciones IP dinámicas fuera necesario para proteger el buen funcionamiento de los servicios de Internet frente a eventuales ataques. No creo que se pueda dar una respuesta en términos absolutos a ese problema, cuya solución, por el contrario, deberá ir precedida, en cada caso singular, del contraste entre el interés del titular del sitio web y los derechos e intereses de los usuarios.

105. En consecuencia, sugiero como respuesta a la segunda pregunta prejudicial que el artículo 7, letra f), de la Directiva 95/46 se opone a una norma nacional cuya interpretación impida a un prestador de servicios recoger y tratar los datos personales de un usuario, al margen de su consentimiento, con el objetivo de garantizar el funcionamiento del servicio de telecomunicación, tras el término de cada operación de uso.

VI. Conclusión

106. En virtud de lo expuesto, propongo al Tribunal de Justicia responder a las cuestiones planteadas en los términos siguientes:

«1) Con arreglo al artículo 2, letra a), de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, una dirección IP dinámica, mediante la que un usuario ha accedido a la página web de un proveedor de servicios de telecomunicaciones, constituye para este último un "dato personal", en la medida en que un proveedor de acceso a la red posea otros datos adicionales que, asociados a la dirección IP dinámica, propicien la identificación del usuario.

2) El artículo 7, letra f), de la Directiva 95/46 debe interpretarse en el sentido de que el objetivo de garantizar el funcionamiento del servicio de telecomunicación puede, en principio, considerarse como un interés legítimo, cuya satisfacción justifica el tratamiento de ese dato personal, sujeto al juicio de su prevalencia sobre el interés o los derechos fundamentales del afectado. Una disposición nacional que no permitiera tomar en cuenta ese interés legítimo sería incompatible con el citado artículo.»