LA PROTECCION DE DATOS A ESCALA EUROPEA EN LA COMPRAVENTA DE ESPACIOS PUBLICITARIOS EN INTERNET: COMBINACION DE LA INFORMACION

ENRIQUE DE MIGUEL CANUTO

SUMARIO

Revista de Derecho Político
N.º 120, mayo, 2024, págs. 335-361
https://doi.org/10.5944/rdp.120.2024.41772

Fecha recepción: 20.12.2023
Fecha aceptación: 20.04.2024

LA PROTECCION DE DATOS A ESCALA EUROPEA EN LA COMPRAVENTA DE ESPACIOS PUBLICITARIOS EN INTERNET: COMBINACION DE LA INFORMACION

ENRIQUE DE MIGUEL CANUTO[1]

Catedrático de Derecho financiero. Universidad de Valencia.

I. PROBLEMATICA

Toda persona tiene derecho a la protección de sus datos de carácter personal[2], calificación relativa al rastro dejado cuando consulta un sitio de Internet o una aplicación informática, cuyo tratamiento debe basarse, nuclearmente, en el consentimiento expresado por la persona afectada, según sabemos recoge la Carta europea de

[1] Facultad de Derecho, Universidad de Valencia, Avenida de los Naranjos s/n, 46022 Valencia. Correo: enrique.de-miguel@uv.es. ORCID ID https://orcid.org/0000-0003-3375-6261 Este trabajo se realiza en el marco del proyecto de investigación «La necesaria actualización de los sistemas tributarios ante los retos del S. xxi», Prometeo/2021/041.

[2] Troncoso Reigada, A., «El marco jurídico de la protección de datos personales: Reglamento UE 2016/679 y Ley Orgánica 3/2018, de 5 de Diciembre», *Revista del Ministerio de Trabajo y Economía Social* nº148, 2021, págs. 23-64; Martínez Villaseca, M., «El interés legítimo como base legitimadora del tratamiento de datos de carácter personal», *Actualidad administrativa* nº 12, 2019; Plaza Penades, J., «Cuestiones básicas del derecho de protección de datos de carácter personal y su seguridad», *Revista Aranzadi de Derecho y Nuevas Tecnologías* nº 63/2023, pp. 1-21; Armada Villaverde, M.E., y Lopez Bustabad, I. J., «El Reglamento general de protección de datos ante el fenómeno del "big data"», *Revista Aranzadi de Derecho y Nuevas Tecnologías* nº 51/2019, pp. 1-34; Dopazo Fraguio, P., «La protección de datos en el derecho europeo: principales aportaciones doctrinales y marco regulatorio vigente (Novedades del Reglamento General de Protección de Datos)», *Revista Española de Derecho Europeo* nº 68/2018pp. 1-16; Arenas Ramiro, M., *El derecho fundamental a la protección de datos personales en Europa* , Valencia, 2006; García-Berrio Hernández, T., *Informática y libertades*: la protección de datos personales y su regulación en Francia y España, Servicio de Publicaciones, Universidad de Murcia, 2003.

Derechos fundamentales, lo que en la actualidad es origen de un rico conjunto de interrogantes.

En el campo de la venta de espacios publicitarios encontramos proveedores de sitios de Internet, intermediarios de datos (*brockers of data*), plataformas publicitarias (*advertising platforms*) y demás empresas de tecnología publicitaria, que pueden tener un conocimiento fragmentario sobre a qué ha consentido o a qué se ha opuesto el usuario de los canales de comunicación electrónica, fragmentos de información cuya composición o combinación puede visibilizar las circunstancias personales identificadoras de la conducta del usuario.

El usuario de servicios de publicidad en línea se encuentra entre dos fuegos: por una parte, los anunciantes, que son los demandantes de espacios de publicidad, sea directamente, sea con la intermediación de agencias de publicidad que actúan en su nombre y por su cuenta, y, por otra parte, los editores de publicidad o anunciadores, que son los oferentes de espacios publicitarios, actuando directamente o con intermediación de proveedores de redes publicitarias o plataformas tecnológicas de publicidad.

El Tribunal de la Unión se ha pronunciado sobre los presupuestos de la responsabilidad del tratamiento de los datos personales por asociaciones internacionales y por empresas o entidades involucradas en los fines y medios de tal actividad de tratamiento, porque las organizaciones empresas y entidades que participan e influyen en las decisiones de determinación de los fines y medios de la actividad de tratamiento de datos pueden ser consideradas responsables.

La problemática relativa a la conservación generalizada e indiferenciada de los datos de tráfico y localización del usuario puede alcanzar incluso la órbita penal, en que debe esclarecerse el valor de las pruebas de cargo con origen en datos conservados sobre tráfico y localización del usuario, desde el punto de vista de las posibilidades reales de contradicción de los que son acusados como participantes en delitos, en el ámbito de los procesos penales.

II. CASO IAB EUROPE

El caso *Interactive Advertising Bureau Europe*[3] , resuelto por sentencia del Tribunal de la Unión de 7 de marzo de 2024, es una cuestión prejudicial elevada por el *Tribunal de apelación* de Bruselas, en relación con la protección de datos en la compraventa en línea de espacios publicitarios[4].

[3] Sentencia del TJUE de 7 de marzo de 2024, caso *Interactive Advertising Bureau Europe*, causa C-604/22, Bélgica.

[4] García Herrero, J., «IAB Europe: corresponsabilidad e ilegalización del marco jurídico de las subastas de publicidad personalizada online (RTB)», *Derecho Digital e Innovación*. Digital Law and Innovation Review, nº 11, 2022.

La actora, IAB Europe, es una asociación sin ánimo de lucro, establecida en Bélgica, que representa a las empresas del sector de la publicidad y del marketing digitales a nivel europeo. Los miembros de IAB Europe son empresas del sector, como editores de publicidad (*publishers*), empresas de comercio electrónico y de marketing e intermediarios, y también asociaciones nacionales, entre ellas las *Interactive Advertising Bureau* (IAB) nacionales, que, a su vez, integran como miembros a empresas del sector. Entre los miembros integrados en la asociación actora, IAB Europe, figuran empresas que generan ingresos importantes mediante la venta de espacios publicitarios en sitios de Internet o en aplicaciones.

El *Transparency & Consent Framework* («TCF») , Marco de Transparencia y Consentimiento, que es un marco de estándares, elaborado por IAB Europe, compuesto por directrices, instrucciones, especificaciones técnicas, protocolos y obligaciones contractuales que permiten tanto al proveedor de un sitio de Internet o de una aplicación como a los intermediarios de datos o incluso a las plataformas publicitarias tratar legalmente los datos personales de un usuario de un sitio de Internet o de una aplicación.

El objetivo del TCF es favorecer el cumplimiento del RGPD de 2016[5] cuando esos operadores recurren al protocolo OpenRTB, uno de los protocolos más utilizados para el *Real Time Bidding*[6], que es un *sistema de subasta en línea instantánea y automatizada de perfiles de usuarios para la compraventa de espacios publicitarios en Internet*[7]. Atendidas determinadas prácticas llevadas a cabo por miembros de IAB Europe en este sistema de intercambio masivo de datos personales relativos a perfiles de usuarios, IAB Europe presentó el Marco TCF como una solución que podía adecuar el sistema de subastas a las exigencias del RGPD de 2016.

Cuando un usuario consulta un sitio de Internet o una aplicación que contiene un espacio publicitario, las empresas de tecnología publicitaria, incluyendo los intermediarios de datos y las plataformas publicitarias, que representan a miles de anunciantes, pueden pujar en tiempo real, sin ser vistos, por la obtención de ese espacio publicitario a través de un sistema de subastas automatizado que utiliza algoritmos,

---

[5] Reglamento 2016/679, del Parlamento y el Consejo, de 27 de abril, Reglamento General de Protección de Datos (*D.O.U.E.* L 119, de 04.05.2016).

[6] En la técnica *Real Time Binding* , los editores de publicidad muestran en plataforma qué espacios publicitarios ponen a la venta , cuál es el precio de venta y qué clase de anunciantes aceptan, al tiempo que los anunciantes compran en función del perfil conductual del usuario, la ubicación del formato, la hora del día y la zona geográfica e indican qué precio están dispuestos a pagar (Aviño Belenguer, D., «El uso de cookies de publicidad comportamental desde la óptica de la protección de datos» , *Revista Aranzadi de Derecho y Nuevas Tecnologías* nº 56, 2021, p. 6).

[7] Otras formas de compraventa programática de publicidad se pueden hacer a través de las *ad exchanges*-donde editores y anunciantes se ponen en contacto —o de las plataformas tecnológicas de publicidad (*sell side platform*), mediante subasta abierta, subasta privada, acuerdo preferente o *programatic* garantizado (Aviño Belenguer, D., «El uso de cookies de publicidad comportamental desde la óptica de la protección de datos» , *Revista Aranzadi de Derecho y Nuevas Tecnologías* nº 56, 2021, p. 5).

con el fin de mostrar en el espacio publicidad dirigida adaptada específicamente al perfil[8] de tal usuario.

Antes de mostrar esa publicidad dirigida, debe obtenerse el consentimiento[9] del usuario. Cuando éste consulta un sitio de Internet por primera vez, una plataforma de gestión del consentimiento, «Consent Management Platform» («CMP»)[10], aparece en una ventana emergente que permite al usuario, bien dar su consentimiento al proveedor del sitio de Internet para la recogida y el tratamiento de sus datos personales con fines previamente definidos -como la comercialización o la publicidad- o para el intercambio de esos datos con determinados proveedores, bien oponerse a diferentes clases de tratamiento de datos o al intercambio de estos datos sobre la base de los *intereses legítimos*[11] que pueden invocar los proveedores en el sentido del artículo 6, apartado 1, letra f), del RGPD de 2016. Estos datos personales se refieren a la localización del usuario, su edad, su historial de búsquedas y sus compras recientes.

En este contexto, el TCF proporciona un marco para un tratamiento de datos personales a gran escala y facilita el registro de las preferencias de los usuarios a través de la plataforma CMP. A continuación, estas preferencias se codifican y almacenan en una cadena compuesta por una combinación de letras y caracteres, designada como **Transparency and Consent String** («TC String»), que se comparte con intermediarios de datos personales y plataformas publicitarias que participan en el protocolo OpenRTB, para que estos sepan en qué ha consentido el usuario o a qué se ha opuesto. La Plataforma de Gestión del Consentimiento coloca también una cookie «euconsent-v2» en el dispositivo del usuario. Cuando se combinan, la

[8] Se trata del perfil conductual o «perfil de personalidad» sobre gustos, expectativas e intereses del usuario deducidos de rastrear sus movimientos.

[9] Sobre las distintas fórmulas de información y de consentimiento que utilizan las empresas implicadas en el sector de la publicidad puede verse Aviño Belenguer, D., «El uso de cookies de publicidad comportamental desde la óptica de la protección de datos», *Revista Aranzadi de Derecho y Nuevas Tecnologías* nº 56, 2021, pp. 1-31. También Polo Roca, A., «El derecho a la protección de datos personales y su reflejo en el consentimiento del interesado», *Revista de Derecho Político* nº 108, 2020, pp. 165-194 y Morales Barcelo, J., «Big data y protección de datos: especial referencia al consentimiento del afectado», *Revista Aranzadi de Derecho y Nuevas Tecnologías* nº 44, 2017, pp. 1-25.

[10] Una Plataforma de Gestión de consentimiento es una herramienta que se instala en el soporte del editor de publicidad, página web o aplicación informática y facilita que cualquier editor de publicidad o tercero responsables de la utilización de cookies cumpla sus deberes de información y recogida del consentimiento del usuario, en cuyo caso responderá directa e individualmente frente al usuario en relación a la obligación de obtener el consentimiento (Aviño Belenguer, D., «El uso de cookies de publicidad comportamental desde la óptica de la protección de datos» , *Revista Aranzadi de Derecho y Nuevas Tecnologías* nº 56, 2021, p. 18).

[11] El artículo 6, apartado 1, letra f), del RGPD de 2016 enuncia un juicio de ponderación entre los intereses legítimos en el tratamiento de datos y los derechos fundamentales del usuario objeto de protección. Su problemática aflora con toda nitidez en la sentencia del TJUE de 19 de octubre de 2016, caso *Patrick Breyer*, causa C-582/14, que es analizada en el epígrafe VIII de este trabajo.

cadena TC String y la cookie[12] euconsent-v2 pueden vincularse a la dirección IP de ese usuario.

De este modo, el Marco TCF desempeña un papel en el funcionamiento del protocolo OpenRTB, ya que permite transcribir las preferencias del usuario para su comunicación a potenciales vendedores y alcanzar diferentes objetivos de tratamiento, incluido ofrecer publicidad a medida. El TCF tiene por objeto garantizar a los intermediarios de datos personales y a las plataformas publicitarias el cumplimiento del RGPD de 2016 a través de la cadena TC String.

La Autoridad de Protección de Datos (APD) de Bélgica, desde 2019, había recibido varias denuncias contra la actora, en relación con la disconformidad del Marco TCF con el RGPD de 2016. En su condición de autoridad de control principal, activó el mecanismo de cooperación y coherencia, con el fin de llegar a una decisión común aprobada conjuntamente por las veintiuna Autoridades de control nacionales. Así, la **Sala de Controversias** de la APD, mediante resolución de 2 de febrero de 2022, declaró que la actora era responsable del tratamiento de los datos personales en relación con el registro del consentimiento, de las objeciones y de las preferencias de los usuarios individuales a través de una cadena TC String, la cual, según la Sala, está asociada a un usuario identificable. La Sala ordenó a la actora, según el artículo 100, apartado 1, punto 9.º, de la Ley APD, que adecuara a las disposiciones del RGPD de 2016 el tratamiento de datos personales efectuado en el marco del TCF y le impuso varias medidas correctoras y una *multa administrativa*.

La actora interpuso recurso contra la resolución ante el **Tribunal de Apelación de Bruselas**, Bélgica, que es el tribunal remitente, solicitando que se anule la resolución de 2022. Se opone a que se considere que actuó como responsable del tratamiento. Sostiene que, la resolución no está suficientemente motivada y que, en todo caso, es errónea. Subraya que solo los demás participantes en el Marco TCF podrían combinar la cadena TC String con una dirección IP para transformarla en un dato personal, que la cadena TC String no es específica de un usuario y que ella no tiene la posibilidad de acceder a los datos tratados en este contexto por sus miembros.

La Autoridad belga sostiene que las cadenas TC Strings contienen datos personales, porque las Plataformas CMP pueden vincular las cadenas TC Strings a las direcciones de protocolo de internet, que, además, los participantes en el Marco TCF también pueden identificar a los usuarios sobre la base de otros datos, que la actora tiene acceso a la información requerida, siendo esta identificación del usuario la finalidad de la cadena TC String, mediante la cual se pretende *facilitar la venta de la publicidad dirigida*.

Que IAB Europe deba ser considerada responsable del tratamiento en el sentido del RGPD de 2016 se desprende de su función determinante en el tratamiento de

[12] Como es sabido la cookie es un dispositivo de almacenamiento y recuperación de datos del usuario ubicado de ordinario en el equipo terminal del usuario por un proveedor de red. En este contexto se trata de las cookies de publicidad conductual, para la elaboración de perfiles.

las cadenas TC Strings. Tal organización determina los fines y los medios del tratamiento, el modo en que se generan, modifican y leen las cadenas TC Strings, de qué manera y dónde se almacenan las cookies necesarias, quién recibe los datos personales y sobre la base de qué criterios pueden establecerse los plazos de conservación de las TC String.

El Tribunal remitente en síntesis se interroga sobre si una cadena TC String, combinada o no con una dirección IP, debe ser considerada un dato personal y, de ser así, si la actora debe ser calificada de responsable del tratamiento de los datos personales en el marco del TCF, en relación con el tratamiento de la cadena TC String. Si bien es cierto que la resolución de 2022 refleja la posición común adoptada conjuntamente por las autoridades de control nacionales implicadas, el Tribunal de la Unión no había tenido ocasión de pronunciarse sobre esta nueva tecnología intrusiva, TC String.

III. CADENA DE DATOS TRATADOS

El Tribunal remitente pregunta si el artículo 4, punto 1, del RGPD de 2016 debe interpretarse en el sentido de que una cadena compuesta por una combinación de letras y caracteres, como la TC String, que contiene las preferencias de un usuario de Internet o de una aplicación relativas al consentimiento del usuario en el tratamiento de datos personales por proveedores de sitios de Internet o de aplicaciones, así como por intermediarios de datos y por plataformas publicitarias, debe considerase contiene datos personales, cuando una organización sectorial ha establecido el marco de estándares para la generación, almacenamiento y difusión de la cadena de datos y los miembros de la organización han aplicado tales estándares y tienen así acceso a la cadena[13].

Se interroga acerca de si tiene relevancia para la solución del caso que la cadena esté asociada a un identificador, como la dirección de protocolo de internet del dispositivo del usuario, que permite identificar al interesado, y, también, si la tiene que la organización disponga del derecho a acceder directamente a los datos personales tratados por sus miembros en el contexto del marco de estándares que ella ha establecido.

Partimos de que el artículo 4, punto 1, del RGPD de 2016 indica que debe considerarse dato personal «toda información sobre una persona física identificada o identificable» y que «se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la

[13] Apartado nº 32 y ss. de la sentencia del TJUE de 7 de marzo de 2024, caso Interactive Advertising Bureau Europe, causa C-604/22.

identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona».

La expresión «toda información» en la definición del concepto de «datos personales», evidencia el *objetivo* del legislador de la Unión de atribuir a este concepto un *significado amplio*, que puede abarcar todo género de información, tanto objetiva como subjetiva, en forma de opiniones o apreciaciones, siempre que sea información «sobre» la persona en cuestión. El Tribunal de la Unión ha declarado que una información se refiere a una persona física identificada o identificable cuando, debido a su contenido, finalidad o efectos, la información está relacionada con una persona identificable (sentencia de 4 de mayo de 2023, caso Österreichische Datenschutzbehörde y CRIF, causa C-487/21, apartados 23 y 24).

En cuanto al carácter «identificable» de una persona, de la redacción del artículo 4, punto 1, del RGPD de 2016 se desprende que no solo es persona identificable aquella que puede ser identificada directamente, sino también la que puede ser identificada indirectamente.

El uso del término «indirectamente» muestra que, para calificar una información de dato personal, no es necesario que la información permita, por sí sola, identificar al interesado (sentencia de 19 de octubre de 2016, caso *Patrick Breyer*[14], causa C-582/14, apartado 41). Al contrario, del artículo 4, punto 5, del RGPD, en relación con el considerando 26 del Reglamento de 2016, se desprende que los datos personales que cabría atribuir a una persona física mediante la utilización de información adicional deben considerarse información sobre una persona física identificable (sentencia de 5 de diciembre de 2023, caso Nacionalinis visuomenės sveikatos centras, causa C-683/21, apartado 58).

Por otra parte, según el Considerando 26 del Reglamento, para determinar si una persona es «identificable», deben tenerse en cuenta «todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física». El enunciado sugiere que, para que un dato pueda ser calificado de «dato personal», en el sentido del artículo 4, punto 1, del Reglamento de 2016, no es necesario que toda la información que permita identificar al interesado se encuentre en poder de una sola persona (sentencia de 19 de octubre de 2016, caso Patrick *Breyer*, causa C-582/14, apartado 43).

Siendo así, el concepto de «datos personales» no abarca únicamente los datos recabados y conservados por el responsable del tratamiento, sino que incluye también todas las informaciones resultantes de un tratamiento de datos personales que se refieran a una persona identificada o identificable (sentencia de 22 de junio de 2023, *caso Pankki S*, causa C-579/2, apartado 45).

En el caso de autos, una cadena compuesta por una combinación de letras y caracteres, como la TC String, contiene las preferencias de un usuario de Internet o de

[14] *Ut infra*, epígrafes VI, VII, VIII y IX de este trabajo.

una aplicación relativas al consentimiento del usuario en el tratamiento por terceros de datos personales o que se refieren a su eventual oposición a un tratamiento de los datos basado en un interés legítimo alegado según el artículo 6, apartado 1, letra f), del RGPD de 2016.

Aun cuando una TC String no contiene en sí misma elementos que permitan la identificación directa del interesado, no es menos cierto, en primer lugar, que contiene las preferencias individuales de un usuario específico en cuanto a su consentimiento en el tratamiento de sus datos personales, lo que supone información «sobre una persona física», en el sentido del artículo 4, punto 1, del RGPD de 2016.

En segundo lugar, y ésta es la *ratio decidendi*, también consta *que, cuando la información contenida en una cadena TC String se asocia con un identificador, como la dirección de protocolo de internet del dispositivo de tal usuario, puede permitir crear un perfil conductual de dicho usuario e identificar efectivamente a la persona a que se refiere específicamente tal información*.

En cuanto que el asociar una cadena, como la TC String, con datos adicionales, como la dirección de protocolo de internet del dispositivo de un usuario o con otros identificadores, permite identificar al usuario, debe considerarse que la cadena TC String contiene información sobre un usuario identificable, lo que supone conocer un dato personal, en el sentido del artículo 4, punto 1, del RGPD, lo que viene corroborado por el considerando 30 del RGPD de 2016, que se refiere a este supuesto.

No cambia la conclusión por la circunstancia de que la propia actora no pueda combinar la cadena TC String con la dirección de protocolo de internet del dispositivo del usuario y no tenga la posibilidad de acceder directamente a los datos tratados por sus miembros. Como se desprende de la jurisprudencia mencionada, esta circunstancia no impide que una cadena TC String sea calificada de «dato personal», en el sentido del artículo 4, punto 1, del RGPD de 2016. Por lo demás, de la resolución de la Sala de Conflictos de 2022, se desprende que los miembros de IAB Europe están obligados a comunicar a la actora, a petición de esta, la información que le permita identificar a los usuarios cuyos datos son objeto de una cadena TC String.

A la luz de lo expuesto en el considerando 26 del RGPD de 2016, resulta que la actora dispone de medios razonables que le permiten identificar a una persona física determinada a partir de una cadena TC String, gracias a la información que sus miembros y otras organizaciones que participan en el Marco TCF[15] están obligados a facilitarle. Por lo que una TC String es un dato personal en el sentido del artículo 4, punto 1, del RGPD.

En tal sentido, carece de relevancia que, sin una contribución externa, tal organización sectorial no pueda acceder a los datos tratados por sus miembros en el marco de los estándares establecidos, ni combinar la cadena TC String con otros

[15] El «TCF», Marco de Transparencia y Consentimiento, como hemos visto, es el marco de estándares, elaborado por la asociación actora, que permiten a los proveedores de un sitio de Internet, a los intermediarios de datos y a las plataformas publicitarias el tratamiento de los datos del usuario.

identificadores, como la dirección de protocolo de internet del dispositivo de un usuario, atendido que puede exigir esa información a sus miembros.

En suma, el artículo 4, punto 1, del RGPD de 2016 debe interpretarse en el sentido de que una cadena, como la TC String, que contiene las preferencias de un usuario de Internet o relativas al consentimiento del usuario en el tratamiento de sus datos personales por proveedores de sitios de Internet, así como por intermediarios de tales datos y por plataformas publicitarias, contiene un dato personal, en cuanto que, cuando puede asociarse, por medios razonables, a un identificador, como la dirección de protocolo de internet del dispositivo de dicho usuario, permite identificar al interesado.

IV. RESPONSABLE DEL TRATAMIENTO

¿Quién es, en este contexto, responsable del tratamiento de los datos personales? El Tribunal remitente también pregunta si a luz del artículo 4, punto 7 del RGPD de 2016, una organización sectorial debe ser considerada «responsable del tratamiento», en cuanto propone a sus miembros un marco de estándares en materia de consentimiento en el tratamiento de datos personales, que contiene no solo estándares técnicos vinculantes, sino también estándares que precisan de manera detallada las modalidades de almacenamiento y de difusión de los datos personales relativos al consentimiento.[16]

Debemos partir de que el objetivo perseguido por el RGPD de 2016, tal como se desprende de su artículo 1 y de sus considerandos 1 y 10, consiste en garantizar un nivel elevado de protección de los derechos y libertades fundamentales de las personas físicas, sobre todo de su *derecho a la vida privada*[17] respecto del tratamiento de los datos personales, consagrado en el artículo 8, apartado 1, de la Carta y en el artículo 16 TFUE, apartado 1[18]. Conforme a este objetivo, el artículo 4, punto 7, del Reglamento de 2016 define, de manera amplia, el concepto de «responsable del tratamiento» como la persona física o jurídica, autoridad pública, servicio u otro

[16] Apartado nº 52 y ss. de la sentencia del TJUE de 7 de marzo de 2024, caso Interactive Advertising Bureau Europe, causa C-604/22.

[17] El derecho fundamental a la protección de los datos de carácter personal, recogido en el artículo 8 de la Carta europea de derechos fundamentales, encuentra su fundamento en el derecho al respeto de la vida privada reconocido en el artículo 7 de la misma Carta, que, a su vez, está en correspondencia con el artículo 8 del C.E.D.H., sobre derecho a la vida privada. Episodio expresivo de la interacción TEDH-TJUE en este campo es la sentencia del TEDH de 30 enero de 2020, rec. 50001/12, caso Breyer / Alemania, con el voto particular del juez Ranzoni. Puede verse Rodríguez Lainz, J.L., «Sobre la licitud de regímenes legales de conservación de datos identitarios de tarjetas de telefonía prepago (a propósito de la STEDH del Caso Breyer v. Alemania)», *Diario La Ley*, nº 9774, 2021.

[18] Sentencia de 4 de mayo de 2023, caso Bundesrepublik Deutschland (Buzón electrónico judicial), causa C-60/22, apartado 64.

organismo que, solo o junto con otros, determine los fines y medios del tratamiento de datos personales.

En efecto, tal como ya ha declarado el Tribunal de la Unión, el objetivo de esta disposición consiste en garantizar, mediante una definición amplia del concepto de «responsable del tratamiento», una protección eficaz y completa de los interesados (sentencia de 5 de junio de 2018, caso Wirtschaftsakademie Schleswig-Holstein, causa C-210/16, apartado 28).

Puesto que, tal como prevé el artículo 4, punto 7, del RGPD de 2016, el concepto de «responsable del tratamiento» se refiere al organismo que «solo o junto con otros» determine los fines y los medios del tratamiento de datos personales, dicho concepto no se remite necesariamente a una única entidad, sino que puede aludir a varios actores que participen en ese tratamiento, cada uno de los cuales estará por tanto sujeto a las disposiciones aplicables en materia de protección de datos (sentencias de 5 de junio de 2018, caso Wirtschaftsakademie Schleswig-Holstein, causa C-210/16, apartado 29, y de 10 de julio de 2018, caso Jehovan todistajat, causa C-25/17, apartado 65).

El Tribunal de la Unión ha considerado *que una persona física o jurídica que, atendiendo a sus propios objetivos, influye en la actividad de tratamiento de datos personales y participa, por ello, en la determinación de los fines y los medios del tratamiento puede ser considerada responsable del tratamiento* en el sentido del artículo 4, punto 7, del RGPD de 2016 (sentencia de 10 de julio de 2018, caso Jehovan todistajat, causa C-25/17, apartado 68). Así, a la luz del artículo 26, apartado 1, del RGPD de 2016, existen «corresponsables del tratamiento» cuando dos o más responsables del tratamiento determinen conjuntamente los fines y medios del tratamiento (sentencia de 5 de diciembre de 2023, caso Nacionalinis visuomenės sveikatos centras, causa C-683/21, apartado 40).

Si bien cada corresponsable del tratamiento debe responder de manera independiente como «responsable del tratamiento» del artículo 4, punto 7, del RGPD de 2016, la concurrencia de una responsabilidad conjunta no supone necesariamente que, con respecto a una misma actividad de tratamiento de datos personales, los diversos agentes tengan una responsabilidad equivalente. Bien al contrario, *los agentes o participantes pueden estar implicados en distintas etapas de la actividad de tratamiento y en distintos grados*, de modo que el nivel de responsabilidad de cada uno debe evaluarse teniendo en cuenta todas las circunstancias relevantes del caso. Además, la responsabilidad conjunta de varios agentes respecto a una misma actividad de tratamiento no exige que todos y cada uno de ellos pueda conocer los datos personales[19]. (sentencia de 10 de julio de 2018, caso Jehovan todistajat, causa C-25/17, apartados 66 y 69).

La participación en la determinación de los fines y medios de la actividad de tratamiento puede adoptar distintas formas y resultar tanto de una decisión común

[19] En este sentido, sentencia de 5 de junio de 2018, caso *Wirtschaftsakademie* Schleswig-Holstein, causa C-210/16, apartado 38, sentencia de 10 de julio de 2018, caso Jehovan todistajat, causa C-25/17, apartado 66 y 69 y sentencia de 29 de julio de 2019, caso Fashion ID, causa C-40/17, apartado 69.

adoptada por dos o más entidades como de decisiones convergentes de las entidades. Tales decisiones deben complementarse, de modo que cada una de ellas tenga un efecto concreto en la determinación de los fines y medios del tratamiento. En cambio, no puede circunscribirse al caso de que exista un acuerdo formal entre los responsables del tratamiento en cuanto a los fines y medios del tratamiento[20] .

Proyectándolo en el caso vemos que la primera parte de la cuestión planteada tiene por objeto que se determine si una organización sectorial, como IAB Europe, puede ser considerada corresponsable del tratamiento, en el sentido de los artículos 4, punto 7, y 26, apartado 1, del RGPD de 2016. Para ello, es preciso apreciar si dicha organización sectorial influye, atendiendo a sus propios objetivos, en el tratamiento de datos personales, como la cadena TC String, y determina, junto con otros, los fines y medios de tal tratamiento.

En primer lugar, en cuanto a los fines de tal tratamiento de datos personales, de los autos se desprende que el TCF establecido por IAB Europe constituye un marco de estándares que tiene por objeto garantizar la conformidad con el RGPD de 2016 del tratamiento de datos personales de un usuario de un sitio de Internet o de una aplicación efectuado por determinados operadores que participan en la subasta en línea de espacios publicitarios.

En estas circunstancias, el Marco TCF pretende favorecer y permitir la compraventa de espacios publicitarios en Internet por parte de esos operadores. Por consiguiente, puede considerarse, que IAB Europe influye, atendiendo a sus propios objetivos, en las operaciones de tratamiento de datos personales y determina, junto con sus miembros, los fines de tales operaciones.

En segundo lugar, en cuanto a los medios utilizados para tal tratamiento de datos personales, de los autos se desprende, que el TCF constituye un marco de estándares que los miembros de IAB Europe deben aceptar para adherirse a la asociación. Como confirmó la actora en la vista, si alguno de sus miembros no cumple los estándares del TCF, la actora puede adoptar respecto de ese miembro una *decisión de incumplimiento* y de suspensión que puede dar lugar a la exclusión de dicho miembro del TCF, y, por lo tanto, a impedirle invocar la garantía de conformidad con el RGPD de 2016 que supuestamente proporciona ese dispositivo para el tratamiento de datos personales que efectúa mediante cadenas TC Strings.

Además, y desde un punto de vista práctico, el Marco TCF establecido por la actora contiene especificaciones técnicas, que describen con precisión el modo en que las CMP[21] están obligadas a recabar las preferencias de los usuarios en relación con el tratamiento de los datos personales que les conciernen y la manera en que deben

[20] Sentencia de 5 de diciembre de 2023, caso Nacionalinis visuomenės sveikatos centras, causa C-683/21, apartados 43 y 44.

[21] Las plataformas de Gestión de consentimiento (*Consent Management Platform*) son herramientas informáticas que se instalan en el soporte del editor de publicidad o página web y facilitan que el editor cumpla sus deberes de recogida previa información del consentimiento del usuario afectado por la actividad de tratamiento de datos.

tratarse tales preferencias para generar una cadena TC String. También se establecen normas precisas en lo que respecta al contenido de la cadena TC String, así como al almacenamiento y al intercambio de esta.

Se desprende en concreto de la resolución de 2022 que la actora prescribe, en el marco de estas normas, el modo normalizado en que las diferentes partes implicadas en el Marco TCF pueden consultar las preferencias, las objeciones y los consentimientos de los usuarios contenidos en las cadenas TC Strings.

En estas circunstancias, debe considerarse que una organización sectorial como la actora influye, atendiendo a sus propios objetivos, en las operaciones de tratamiento de datos personales y determina, junto con sus miembros, los medios que están en el origen de tales operaciones. De lo que se deduce que debe ser considerada «corresponsable del tratamiento», en el sentido de los artículos 4, punto 7, y 26, apartado 1, del RGPD de 2016, de conformidad con la jurisprudencia mencionada.

Que la propia organización sectorial no tenga acceso directo a las cadenas TC Strings y, por tanto, a los datos personales tratados en el marco de dichos estándares por sus miembros, junto con los cuales determina los fines y medios del tratamiento de esos datos, no impide, de conformidad con la jurisprudencia indicada, que pueda ser calificada de «responsable del tratamiento».

La respuesta dada por el Tribunal de la Unión a la cuestión prejudicial, en conjunto, por las razones expuesta, conduce hacia el mantenimiento de las medidas correctoras y la multa administrativa impuesta por la Sala de controversias de la Autoridad belga de protección de datos a la actora como responsable de la actividad del tratamiento de los datos personales

V. ALCANCE DE LA RESPONSABILIDAD

En respuesta a las dudas expresadas por el Tribunal de remisión, caso *IAB Europe*, el Tribunal de la Unión entiende que debe excluirse que la eventual corresponsabilidad de esta organización sectorial se extienda automáticamente a los tratamientos ulteriores de datos personales efectuados por terceros, tales como los proveedores de sitios de Internet o de aplicaciones, en lo que respecta a las preferencias de los usuarios, a efectos de la publicidad dirigida en línea[22].

Señala que el artículo 4, punto 2, del RGPD define el «tratamiento» de datos personales como «cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o

[22] Apartado nº 40 y ss. de la sentencia del TJUE de 7 de marzo de 2024, caso Interactive Advertising Bureau Europe, causa C-604/22.

interconexión, limitación, supresión o destrucción». De esta definición resulta que un tratamiento de datos personales puede estar constituido por una o varias operaciones, cada una de ellas referida a una de las distintas fases del tratamiento.

Por otro lado, como ha declarado el Tribunal de la Unión, de los artículos 4, punto 7, y 26, apartado 1, del RGPD se desprende que una persona física o jurídica únicamente puede ser considerada corresponsable de las operaciones de tratamiento de datos personales si determina conjuntamente los fines y medios. Por consiguiente, y sin perjuicio de una eventual responsabilidad civil[23] prevista en el Derecho nacional, cuando sea el caso, dicha persona física o jurídica *no puede ser considerada responsable, de las operaciones anteriores o posteriores de la cadena de tratamiento respecto de las que no determine los fines ni los medios* (sentencia de 29 de julio de 2019, caso *Fashion ID*[24], causa C-40/17, apartado 74).

En el presente caso, debe distinguirse entre, por una parte, el tratamiento de datos personales efectuado por los miembros de IAB Europe, a saber, los proveedores de sitios de Internet o de aplicaciones y los intermediarios de datos o incluso las plataformas publicitarias, en el momento del registro en una cadena TC String de las preferencias en materia de consentimiento de los usuarios según el marco de estándares establecido en el TCF y, por otra parte, el *tratamiento ulterior* de datos personales efectuado por esos operadores y por terceros, tales como los proveedores de sitios de Internet o de aplicaciones, sobre la base de tales preferencias, como la transmisión de esos datos a terceros o la oferta de publicidad personalizada dirigida a dichos usuarios.

Este tratamiento ulterior, sin perjuicio de las comprobaciones que corresponde efectuar al Tribunal remitente, *a priori* no prejuzga la participación de IAB Europe, de modo que debe excluirse atribuir automáticamente una responsabilidad a tal organización, junto con dichos operadores y con terceros, en lo que respecta al tratamiento de los datos personales efectuado después sobre la base de los datos relativos a las preferencias de los usuarios que se contienen en una cadena TC String.

En suma, según el Tribunal de la Unión, una organización sectorial, como IAB Europe, solo puede ser considerada responsable de tales tratamientos ulteriores si se demuestra que ha influido en la determinación de los fines de los tratamientos y de las modalidades de su ejercicio, extremo que corresponde comprobar al tribunal remitente a la luz de todas las circunstancias relevantes en el litigio.

---

[23] Se tratará de una eventual responsabilidad por resultado derivada de los daños causados a la intimidad de la persona física, por la entidad actuante, cuando exista una relación de causalidad entre la actividad realizada y el resultado producido. Puede verse Gil González, E., «¿Qué implicaciones tiene insertar en una página web el botón «me gusta» de Facebook? Análisis y comentarios de la sentencia TJUE en el caso Fashion ID», *La Ley privacidad* nº 2, 2019.

[24] La ejemplar sentencia del TJUE de 29 de julio de 2019, caso *Fashion ID*, causa C-40/17, Alemania, ponente Rosas, es una cuestión prejudicial elevada por el *Oberlandesgericht* de Dusseldorf, en que la empresa actora, en su página web inserta un código de programación —el módulo «me gusta de Facebook— que lleva a que el navegador del usuario, al solicitar contenidos al proveedor del módulo, transmita datos personales del usuario al proveedor del módulo.

VI. CASO PATRICK BREYER

El anterior caso *Patrick Breyer*[25], resuelto por sentencia del Tribunal de la Unión de 19 de octubre de 2016, es una cuestión prejudicial elevada por el *Bundesgerichtshof* de Alemania, sobre la dirección de protocolo de Internet dinámica y la garantía del funcionamiento del servicio[26].

El actor, el Sr. Breyer, consultó varios sitios de Internet, accesibles al público, de organismos federales en Alemania, que suministran información actualizada. Para prevenir ataques y posibilitar el ejercicio de acciones penales contra los «piratas», esos sitios registran las consultas en ficheros de protocolo. Al final de la sesión de consulta, en ellos se conservan el nombre del sitio o fichero consultado, los términos introducidos en los campos de búsqueda, la fecha y hora de la consulta, la cantidad de datos transmitidos, la constatación del éxito de la consulta y la dirección IP del ordenador desde el que se ha realizado la consulta.

Las direcciones IP son secuencias de números que se asignan a los ordenadores conectados a Internet, para que estos puedan comunicarse entre sí a través de esa red. Cuando se consulta un sitio de Internet, la dirección IP del ordenador que consulta se comunica al servidor en el que se aloja el sitio consultado. Dicha comunicación es necesaria para que los datos consultados puedan transferirse al destinatario[27].

Por otro lado, los ordenadores de los usuarios de Internet reciben de los proveedores de acceso a Internet una dirección IP «estática» o una dirección IP «dinámica», es decir, una dirección IP que cambia con ocasión de cada nueva conexión a Internet. A diferencia de las direcciones IP estáticas, las direcciones IP dinámicas no permiten relacionar, mediante ficheros accesibles al público, un ordenador concreto y la conexión física a la red utilizada por el proveedor de acceso a Internet.

El actor presentó, ante los tribunales de lo contencioso-administrativo alemanes, recurso con objeto de que se prohibiera en Alemania conservar o permitir que terceros conservasen, al final de las sesiones de consulta de sitios accesibles al público de medios en línea de organismos federales alemanes, la dirección IP del sistema principal de acceso del actor, en la medida en que dicha conservación no fuera necesaria, en caso de fallo, para el restablecimiento de la difusión de esos medios. Recurso que fue desestimado.

---

[25] Sentencia del TJUE de 19 de octubre de 2016, caso Patrick Breyer, causa C-582/14, Alemania, ponente Rosas.

[26] Puede verse Pautrot, B., « Adresse IP : victoire du relativisme sur les dogmatismes quant à la qualification de données à caractère personnel», *Droit de l'immatériel* nº 134, 2017, pp. 23-29.

[27] Protocolo, en este contexto, es el conjunto de estándares que ordenan el establecimiento mantenimiento y cancelación entre dispositivos de una red. *Internet Protocol* (IP) es el Protocolo de nivel 3, que contiene información de dirección y control, para el encaminamiento de los paquetes de datos a través de la red. Las direcciones IP son códigos numéricos, únicos, que identifican la red en que se está operando e identifican un ordenador concreto dentro de esa red, ordenador conectado a la red Internet, que usa el protocolo IP.

Contra la resolución desestimatoria de su recurso en primera instancia, el actor interpuso recurso de apelación. El tribunal de apelación modificó parcialmente la resolución y condenó al Estado alemán a abstenerse de conservar o permitir que terceros conservasen, al final de cada consulta, la dirección IP del sistema principal de acceso del actor, transmitido durante la consulta por éste, de sitios accesibles al público de medios en línea de organismos federales alemanes, cuando dicha dirección se conserva en combinación con la fecha de la sesión de consulta y cuando el actor ha revelado su identidad durante la sesión, también bajo la forma de una dirección electrónica que mencione su identidad, en la medida en que dicha conservación no sea necesaria, en caso de fallo, para el restablecimiento de la difusión del medio en línea.

Según el tribunal de apelación, una dirección IP dinámica, en combinación con la fecha de la sesión de consulta, supone, cuando el usuario del sitio de Internet ha revelado su identidad durante esa sesión, un dato personal, porque el operador de ese sitio puede identificar al usuario cruzando su nombre con la dirección IP de su ordenador. Sin embargo, el tribunal consideró que no procedía estimar el recurso en los demás casos. Cuando el actor no indica su identidad durante una sesión de consulta, sólo el proveedor de acceso a Internet podría relacionar la dirección IP con un abonado identificado. En cambio, atendida su condición de proveedor de servicios de medios en línea, la dirección IP en poder del Estado alemán, no es un dato personal, ni siquiera en combinación con la fecha de la sesión de consulta, puesto que el usuario de los sitios de Internet no es identificable por el Estado.

VII. CRITERIO OBJETIVO Y CRITERIO RELATIVO

Contra la sentencia del tribunal de apelación, caso *Patrick Breyer*, tanto el actor como el Estado alemán interpusieron recursos de casación ante el Bundesgerichtshof, Tribunal Supremo Civil y Penal, que es el tribunal remitente. El actor solicita que se estime íntegramente su pretensión de prohibición. El Estado alemán pide que se desestime la pretensión.

El Tribunal remitente precisa que las direcciones de protocolo de internet dinámicas del ordenador del actor conservadas por el Estado alemán en su condición de *proveedor de servicios* de medios en línea, significan datos concretos sobre circunstancias materiales del actor, atendido que facilitan indicaciones sobre la consulta de determinados sitios o determinados ficheros en Internet en determinadas fechas.

No obstante, según el tribunal remitente, los datos así conservados no permiten determinar directamente la identidad del actor. Los operadores de los sitios de Internet sólo podrían identificar al actor si el *proveedor de acceso* a Internet les transmitiera información sobre la identidad de ese usuario. La calificación de esos datos de «personales» depende, en consecuencia, de si el actor era identificable.

El Tribunal remitente expone la controversia doctrinal relativa a si, para determinar si una persona es identificable, debe tomarse como base un criterio «objetivo» o debe seguirse un criterio «relativo».

Según el criterio **«objetivo»,** datos como las direcciones de protocolo de internet controvertidas, al final de las sesiones de consulta de los sitios de Internet, deben ser calificados como datos personales, aunque solo un tercero pueda determinar la identidad del interesado. Siendo ese tercero, en el presente caso, el proveedor de acceso a Internet del actor, que ha conservado información adicional que permite identificar a éste mediante las mencionadas direcciones de protocolo de internet.

Según el criterio **«relativo»,** tales datos son personales respecto a una entidad como el proveedor de acceso a Internet del actor, porque permiten la identificación precisa del usuario (sentencia de 24 de noviembre de 2011, caso Scarlet Extended, causa C-70/10, apartado 51), pero no lo son respecto a otra entidad como el operador de los sitios de Internet consultados, dado que, en el caso de que el actor no haya revelado su identidad durante las sesiones de consulta, el operador no dispone de la información necesaria para su identificación sin un esfuerzo desmesurado.

En caso de que se considere que las direcciones IP dinámicas del ordenador del actor, en combinación con la fecha de la sesión a la que se refieren, son datos personales, el Tribunal remitente pregunta si la conservación de esas direcciones IP al final de la sesión está autorizada según el artículo 7, letra f), de la Directiva de 95/46[28].

El Bundesgerichtshof precisa que, desde la óptica del Derecho nacional, según el artículo 15, apartado 1, de la TMG, Ley de los servicios electrónicos de comunicación de 2007, los proveedores de servicios de medios en línea sólo pueden recoger y utilizar datos personales de un usuario cuando sea necesario para posibilitar y facturar el uso de esos medios. En Alemania, la conservación de esos datos es necesaria para garantizar la seguridad y la continuidad del buen funcionamiento de los sitios de servicios de medios en línea que ella hace accesibles al público, ya que permiten detectar los «ataques mediante denegación de servicio» , que persiguen paralizar el funcionamiento de los sitios inundando de modo deliberado ciertos servidores de Internet con un gran número de solicitudes, y permiten luchar contra esos ataques.

Según el tribunal remitente, cuando sea necesario que el proveedor de servicios adopte medidas para luchar contra tales ataques, las medidas podrán considerarse necesarias para «posibilitar [...] el uso de los medios electrónicos» según el artículo 15 de la TMG de 2007. Sin embargo, la doctrina defiende mayoritariamente la tesis de que la recogida y utilización de datos personales de un usuario de un sitio de Internet sólo está autorizada para permitir un uso concreto de ese sitio y que esos datos deben ser eliminados al final de la sesión si no son necesarios a efectos de facturación. Para el Tribunal remitente, esta interpretación estricta del artículo 15, apartado 1,

[28] Directiva 95/46 del Parlamento y el Consejo de 24 de octubre de 1995, (*D.O.C.E.* L 281, de 23.11.1995). Puede verse García-Berrio Hernández, T., *Informática y libertades*: la protección de datos personales y su regulación en Francia y España, Servicio de Publicaciones, Universidad de Murcia, 2003.

de la TMG de 2007 se opone a que se autorice la conservación de direcciones IP para garantizar, de modo general, la seguridad y la continuidad del buen funcionamiento de los medios en línea.

El Tribunal remitente se pregunta si esta última interpretación, que es la defendida por el Tribunal de apelación, es conforme con el artículo 7, letra f), de la Directiva 95/46, atendidos los criterios adoptados por el Tribunal de la Unión en la sentencia de 24 de noviembre de 2011, caso ASNEF y FECEMD, causa C-468/10.

VIII. DIRECCIÓN DINÁMICA DE PROTOCOLO DE INTERNET

El Tribunal remitente solicita que se dilucide si el artículo 2, letra a), de la Directiva 95/46, en correspondencia con el artículo 4 punto 1 del RGPD de 2016, debe interpretarse en el sentido de que una dirección IP dinámica registrada por un proveedor de servicios de medios en línea con ocasión de la consulta por una persona de un sitio de Internet que ese proveedor hace accesible al público supone respecto al proveedor, conocer un dato personal, cuando sólo un tercero, en el presente caso el proveedor de acceso a Internet de esa persona, dispone de la información adicional necesaria para identificarla[29].

A tenor de la disposición, se entenderá por «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, mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social.

Con carácter preliminar, debe señalarse que, en la sentencia de 24 de noviembre de 2011, caso Scarlet Extended, causa C-70/10, que se refería a la interpretación de la misma Directiva, el Tribunal de la Unión entendió, que las direcciones de protocolo de internet de los usuarios de Internet son datos protegidos de carácter personal, ya que permiten identificar a esos usuarios. Si bien la afirmación refería a la hipótesis en que la recogida y la identificación de las direcciones de los usuarios de Internet son realizadas por los proveedores de acceso a Internet.

En el presente caso, la cuestión refiere al supuesto en que el proveedor de servicios de medios en línea, el Estado alemán, es quien registra las direcciones IP de los usuarios de sitios de Internet que el prestador de servicios hace accesible al público, sin disponer de la información adicional necesaria para identificar a los usuarios. Además, consta que las direcciones IP a las que se refiere el tribunal remitente son direcciones IP «dinámicas», es decir, provisionales, que se atribuyen en cada conexión a Internet y que son sustituidas en conexiones posteriores, y no direcciones de

[29] Apartado nº 31 y ss. de la sentencia del TJUE de 19 de octubre de 2016, caso Patrick Breyer, causa C-582/14.

protocolo de internet «estáticas», que son invariables y que permiten la identificación permanente del dispositivo conectado a la red.

Por tanto, la cuestión planteada por el tribunal remitente se basa en la **premisa fáctica** de que los datos que consisten en una dirección de protocolo de internet dinámica y en la fecha y hora de la sesión de consulta de un sitio de Internet a partir de dicha dirección IP, registrados por un *proveedor de servicios* de medios en línea no permiten, por sí solos, identificar al usuario que ha consultado el sitio de Internet durante la sesión y, por otro lado, el *proveedor de acceso* a Internet dispone de información adicional que, si se combinara con esa dirección IP, permitiría identificar al usuario[30].

Según el Tribunal de la Unión, cabe comenzar señalando que consta que una dirección de protocolo de internet dinámica en sí misma no constituye una información relativa a una «persona física identificada», pues tal dirección no revela directamente la identidad de la persona física propietaria del ordenador desde el cual se realiza la consulta ni la de otra persona que pudiera utilizar ese ordenador.

A continuación, para determinar si una dirección de protocolo de internet dinámica constituye, desde la premisa fáctica expuesta, un dato personal en el sentido del artículo 2, letra a), de la Directiva 95/46 en relación con el proveedor de servicios de medios en línea, debe analizarse si dicha dirección, registrada por tal proveedor, puede calificarse de información relativa a una «persona física identificable» cuando la información adicional necesaria para identificar al usuario de un sitio de Internet que ese proveedor de servicios hace accesible al público la tiene el proveedor de acceso a Internet de ese usuario.

Del tenor del artículo 2, letra a), de la Directiva 95/46, en correspondencia con el artículo 4 punto 1 del RGPD de 2016, se desprende que se considera identificable a la persona que puede ser identificada no sólo directamente sino también indirectamente. El uso del término «indirectamente» apunta a que, para calificar una información de dato personal, no es necesario que la información permita, por sí sola, identificar al interesado.

Además, el considerando 26 de la Directiva de 1995 enuncia 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. En la medida en que el considerando hace referencia a los medios que puedan ser razonablemente utilizados tanto por el responsable del tratamiento como por «cualquier otra persona», su tenor sugiere que, para que un dato pueda ser calificado de «dato personal», en el sentido del

[30] La doctrina ha señalado el fenómeno de que a los datos recogidos se les aplica algoritmos que, de forma automatizada, llevan a unas correlaciones con vistas a las conclusiones buscadas por quien trata los datos, *correlaciones* que vinculan los datos con una persona determinada, aun cuando no se explicite su identidad por estar asociada a un número o a un código (Morales Barceló, J., «Big data y protección de datos: especial referencia al consentimiento del afectado», *Revista Aranzadi de Derecho y Nuevas Tecnologías* nº 44, 2017, p. 3-4).

artículo 2, letra a), de dicha Directiva, *no es necesario que toda la información que permita identificar al interesado deba encontrarse en poder de una sola persona*.

Que la información adicional necesaria para identificar al usuario de un sitio de Internet no esté en poder del proveedor de servicios de medios en línea, sino del proveedor de acceso a Internet de ese usuario, puede excluir que las direcciones de protocolo de internet dinámicas registradas por el proveedor de servicios supongan, para éste, datos personales en el sentido del artículo 2, letra a), de la Directiva 95/46. No obstante, debe determinarse si la posibilidad de combinar una dirección de protocolo de internet dinámica con tal información adicional en poder del proveedor de acceso es un medio que pueda ser razonablemente utilizado para identificar al interesado.

Como indicó el Abogado General en sus conclusiones, no sucede así cuando la identificación del interesado esté prohibida por la ley o sea prácticamente irrealizable, por ejemplo, porque implique un esfuerzo desmesurado en cuanto a tiempo, costes y recursos humanos, de modo que el riesgo de identificación sea en realidad insignificante.

Aunque el tribunal remitente precisa que el Derecho alemán no permite al proveedor de acceso a Internet transmitir directamente al proveedor de servicios de medios en línea información adicional, necesaria para identificar al interesado, no obstante, existen vías legales que permiten al proveedor de servicios dirigirse, caso de ataques cibernéticos, a la autoridad competente a fin de que ésta lleve a cabo las actuaciones necesarias para obtener la información del proveedor de acceso y para ejercitar acciones penales.

Por tanto, y ésta es la *ratio decidendi* de la cuestión prejudicial, *el proveedor de servicios de medios en línea dispone de medios electrónicos que pueden utilizarse razonablemente para identificar, con ayuda de otras personas, a saber, la autoridad competente y el proveedor de acceso a Internet, al usuario interesado sobre la base de las direcciones de protocolo de internet conservadas*.

En suma, según el Tribunal de la Unión, el artículo 2, letra a), de la Directiva de 1995, en correspondencia con el artículo 4 punto 1 del RGPD de 2016, debe interpretarse en el sentido de que una dirección dinámica de protocolo de internet registrada por un proveedor de servicios de medios en línea con ocasión de la consulta por una persona de un sitio de Internet que ese proveedor hace accesible al público supone respecto a tal proveedor el conocimiento de un dato personal, cuando éste disponga de medios legales que le permitan identificar a la persona interesada gracias a la información adicional de que dispone el *proveedor de acceso* a Internet de dicha persona.

Desde la perspectiva doctrinal acerca de la identificabilidad del usuario, se concluye, por parte del Tribunal de la Unión, el rechazo de la tesis «relativa», para la que la condición del dato personal es afirmada ante un receptor determinado y la suscripción de la tesis «objetiva» , según la cual la condición de dato personal se centra en la potencialidad de identificación del usuario sea por unos o sea por otros receptores de la información.

IX. JUICIO PONDERATIVO ENTRE EL INTERÉS Y LA LIBERTAD

¿Debe efectuarse un juicio ponderativo entre el interés legítimo al tratamiento de los datos y la libertad del usuario objeto de protección?

El Tribunal remitente, caso *Patrick Breyer*, también solicita que se dilucide si el artículo 7, letra f), de la Directiva de 1995, que está en correspondencia con el actual artículo 6.1, letra f) del RGPD de 2016, se opone a una normativa de un Estado en que un proveedor de servicios de medios en línea sólo puede recoger y utilizar datos personales de un usuario, sin el consentimiento de éste, cuando la recogida y utilización sean necesarias para posibilitar y facturar el uso concreto de los servicios por ese usuario, sin que el objetivo de garantizar el funcionamiento general de los servicios pueda justificar la utilización de los datos tras una sesión de consulta de los servicios[31].

Como prolegómeno, debe esclarecerse si el tratamiento de datos personales controvertido, a saber, las direcciones IP dinámicas de los usuarios de sitios de Internet de organismos federales alemanes, debe ser excluido del ámbito de aplicación de la Directiva de 1995, atendido que según el artículo 3, apartado 2, primer guion, la Directiva no se aplica al tratamiento de datos personales que tengan por objeto las actividades del Estado en materia penal. Pues bien, las actividades enumeradas a título de ejemplo en dicha disposición son, en todos los casos, actividades propias del Estado o de las autoridades estatales y ajenas a la esfera de actividades de los particulares[32]. Mientras que, en el presente caso, los organismos federales que prestan servicios de medios en línea y que son responsables del tratamiento de las direcciones IP dinámicas, a pesar de su estatuto de autoridades públicas, *actúan en calidad de particulares*[33] y fuera del ámbito de las actividades del Estado en materia penal.

Por tanto, debe determinarse si una normativa de un Estado como la controvertida en el caso es compatible con el artículo 7, letra f), de la Directiva 95/46. Hemos de partir de que la *normativa nacional*, interpretada en el sentido estricto indicado por el tribunal remitente, sólo autoriza la recogida y utilización de datos personales relativos a un usuario de los servicios, sin consentimiento de éste, en la medida en que sea necesario para posibilitar y facturar el uso concreto del medio en línea, sin que el objetivo de garantizar el funcionamiento general del medio pueda justificar la utilización de esos datos tras una sesión de consulta de ese medio.

---

[31] Apartado nº 50 y ss. de la sentencia del TJUE de 19 de octubre de 2016, caso Patrick Breyer, causa C-582/14.

[32] Sentencias de 6 de noviembre de 2003, caso Lindqvist, causa C-101/01, apartado 43, y de 16 de diciembre de 2008, caso Satakunnan Markkinapörssi y Satamedia, causa C-73/07, apartado 41.

[33] Debemos pues marcar la distinción, a los efectos de la Directiva de 1995, entre la actuación de autoridades públicas en el ejercicio de sus funciones públicas junto a la actuación de autoridades públicas en calidad de particulares y, por otra parte, actuaciones del Estado en materia penal junto a actuaciones en materia de la seguridad pública, la defensa y la seguridad del Estado.

Mientras que según el artículo 7, letra f), de la Directiva de 1995, el tratamiento de datos personales es lícito si «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 artículo 1, apartado 1», de la Directiva.

El Tribunal de la Unión ha declarado que el artículo 7 de la Directiva de 1995 prevé una *lista exhaustiva* y taxativa de los casos en los que un tratamiento de datos personales puede considerarse lícito y que los Estados no pueden añadir 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 el artículo (sentencia de 24 de noviembre de 2011, caso ASNEF y FECEMD[34], causa C-468/10 , apartados 30 y 32).

Si bien el artículo 5 de la Directiva de 1995, que está en correspondencia con el artículo 6.2 de RGPD de 2016, autoriza a los Estados a precisar, dentro de los límites de las disposiciones del capítulo II de la Directiva, y, por tanto, del artículo 7, las condiciones en que son lícitos los tratamientos de datos personales, el *margen de apreciación* de que disponen los Estados en virtud del artículo 5 solamente puede utilizarse de conformidad con el objetivo perseguido por la Directiva, que consiste en mantener un equilibrio entre la libre circulación de datos personales y la tutela del *derecho a la intimidad*[35]. Los Estados no pueden introducir, al amparo del artículo 5 de la Directiva, principios relativos a la legitimación de los tratamientos de datos personales distintos de los enunciados en el artículo 7, ni modificar, mediante exigencias adicionales, el alcance de los seis principios del artículo 7 (sentencia de 24

[34] En el caso ASNEF y FECEMD, causa C-468/10, el Tribunal remitente había preguntado si el artículo 7, letra f), de la Directiva 95/46 —que está en correspondencia con el actual artículo 6.1, letra f) del RGPD de 2016— se opone a una normativa nacional que, en caso de que no concurra consentimiento del interesado , para permitir el tratamiento de datos personales para la satisfacción del interés legítimo buscado por el responsable del tratamiento, exige no sólo que se respeten los derechos y libertades fundamentales del usuario, sino además que los datos figuren en fuentes que sean accesibles al público. La respuesta del Tribunal de la Unión fue que, efectivamente, el Derecho de la Unión se opone a una normativa que en supuesto de que no concurra consentimiento del interesado, exige además de que se respeten los derechos fundamentales, que los datos figuren en fuentes accesibles al público, con lo que está excluyendo de forma categórica y general el tratamiento de datos si éstos no figuran en tales fuentes (Morales Barceló, J., «Big data y protección de datos: especial referencia al consentimiento del afectado», *Revista Aranzadi de Derecho y Nuevas Tecnologías* nº 44, 2017, p.20).

[35] Esta conceptuación supone un método de potenciar la judicialización del ordenamiento y el desapoderamiento del legislador. El sector doctrinal crítico con la ponderación de bienes viene señalando que la ponderación de bienes no proporciona ningún criterio material de los que serían obligados según las exigencias propias del Estado de Derecho relativas a la claridad normativa y seguridad jurídica (Müller, R., *Juristische Methodick*, Berlin, 2ª ed. 1976, p. 53). Crítica en que subyace señalar la ausencia de un criterio real de ordenación social, criterio que es inherente a la norma jurídica en una Unión de Derecho.

de noviembre de 2011, caso ASNEF y FECEMD[36], causa C-468/10, apartados 33, 34 y 36).

En el presente caso, resulta que la norma nacional, el artículo 15 de la TMG de 2007, si recibe la interpretación estricta mencionada por el juez de remisión, tiene un alcance incluso más restrictivo que el principio[37] del artículo 7, letra f), de la Directiva de 1995, que se corresponde con el actual artículo 6.1, letra f) del RGPD de 2016.

En efecto, mientras que el artículo 7, letra f), de la Directiva se refiere, de modo 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 de 2007 sólo autoriza al proveedor de servicios a recoger y utilizar datos personales de un usuario cuando sea necesario para posibilitar y facturar el uso de los medios electrónicos. El artículo 15 de la TMG de 2007 se opone a la conservación, al final de una sesión de consulta de medios en línea, de datos personales para garantizar el uso de esos medios. Sin embargo, los organismos federales que suministran servicios de medios en línea podrían tener también un interés legítimo en garantizar, más allá de cada utilización concreta de sus sitios de Internet accesibles al público, la continuidad del funcionamiento de los sitios.

Como señaló el Abogado General sus conclusiones, tal normativa nacional no se limita a precisar, conforme al artículo 5 de la Directiva de 1995, el concepto de «interés legítimo» que figura en el artículo 7, letra f), de dicha Directiva. Según la jurisprudencia europea el artículo 7, letra f), de la Directiva se opone a que un Estado excluya de manera categórica y generalizada la posibilidad de someter a tratamiento determinadas categorías de datos personales, sin permitir una *ponderación* de los *derechos e intereses en conflicto* en cada caso concreto. Un Estado no puede establecer *a priori* con carácter definitivo el resultado del juicio de ponderación de los derechos e intereses en conflicto respecto de tales categorías, sin permitir un resultado eventualmente diferente en atención a las circunstancias particulares de cada caso concreto (sentencia de 24 de noviembre de 2011, caso ASNEF y FECEMD, causa C-468/10, apartados 47 y 48).

Una normativa como la controvertida, por lo que se refiere al tratamiento de datos personales de los usuarios de sitios de medios en línea, reduce el alcance del principio del artículo 7, letra f), de la Directiva de 1995[38], al excluir que el objetivo

[36] Gimeno, M., «On the direct effect of Article 7 (f) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data», en *Landmark IP Decisions of the European Court of Justice 2008-2013*, Bruselas, 2014 pp. 206-211.

[37] Anotamos que la técnica de ponderación de bienes o principios pone en juego dos bienes o principios, para poder realizar la ponderación, por lo que carece de sentido e induce a confusión, conceptuar como principio el conjunto de elementos que enuncian el propio juicio de ponderación a realizar por el legislador estatal.

[38] Aun cuando el artículo 7 letra f) de la Directiva de 1995 está en correspondencia con el posterior artículo 6.1, letra f) del RGPD de 2016, este último modula que «no será de aplicación

de garantizar el funcionamiento general del medio en línea pueda dar lugar a un juicio de ponderación del interés del responsable del tratamiento y los derechos fundamentales de los usuarios, que requieren una protección según el artículo 1, apartado 1, de la Directiva de 1995[39].

En suma, el artículo 7, letra f), de la Directiva 95/46, que está en correspondencia con el actual artículo 6.1, letra f) del RGPD de 2016, se opone a una normativa según la cual un prestador de servicios sólo puede recoger y utilizar datos personales de un usuario, sin el consentimiento de éste, cuando la recogida y utilización sean necesarias para posibilitar y facturar el uso concreto de los servicios por ese usuario, sin que el objetivo de garantizar el funcionamiento general de esos mismos servicios pueda justificar la utilización de los datos tras una sesión de consulta de los servicios.

Según Aviño Belenguer detrás del conflicto entre el consentimiento y el interés legítimo se encuentra el conflicto entre nuestra privacidad y los beneficios que nos ofrece Internet[40]. Sin embargo, el conflicto entre la intimidad del usuario y los beneficios que le reporta Internet se resuelve en el campo de la expresión del consentimiento del usuario al uso de sus datos, aceptando o rechazando y ese eventual conflicto es ajeno a la ponderación entre el interés legítimo del responsable y la libertad fundamental del usuario.

X. ANOTACIONES CONCLUSIVAS

La jurisprudencia europea ha ido clarificando puntos clave en la definición de qué son datos personales y cuál puede ser su tratamiento, sobresaliendo recientes precisiones aplicadas al campo de la compraventa de espacios publicitarios en línea, espacios en que cotidianamente nos movemos:

1ª que, cuando la información contenida en una cadena de datos, en que se codifica y almacena qué ha consentido y a qué se ha opuesto el usuario de redes de comunicación electrónica, se asocia con un identificador, como la dirección del Protocolo de internet del dispositivo de tal usuario, la combinación puede permitir crear un perfil conductual del usuario e identificar efectivamente a la persona a que se refiere tal información

2ª que una asociación sectorial internacional que influye, atendiendo a sus propios objetivos, en las operaciones de tratamiento de datos personales y

al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones», actividad de tratamiento cuya licitud es amparada por la norma.

[39] Sobre esta problemática, Martínez Villaseca, M., «El interés legítimo como base legitimadora del tratamiento de datos de carácter personal», *Actualidad administrativa* nº 12, 2019; García-Berrio Hernández, T., *Informática y libertades*: la protección de datos personales y su regulación en Francia y España, Servicio de Publicaciones de la Universidad de Murcia, 2003.

[40] Aviño Belenguer, D., «El uso de cookies de publicidad comportamental desde la óptica de la protección de datos» , *Revista Aranzadi de Derecho y Nuevas Tecnologías* nº 56, 2021, p.31.

determina, por ello, junto con sus miembros, los medios electrónicos que están en el origen de tales operaciones, debe ser considerada «corresponsable del tratamiento», en el sentido de los artículos 4, punto 7, y 26, apartado 1, del Reglamento General de Protección de Datos de 2016, de conformidad con la jurisprudencia europea

3ª que una dirección de protocolo de Internet «dinámica»-más volátil que una dirección «estática»- registrada por un *proveedor de servicios* con ocasión de la consulta por una persona de un sitio de Internet o aplicación que ese proveedor hace accesible al público tiene respecto a tal proveedor la consideración de un dato personal, si éste dispone de medios electrónicos que le permitan identificar a la persona interesada gracias a la adición de la información de que dispone sobre la persona el *proveedor de acceso* a Internet

4ª por lo que se refiere al alcance del principio del artículo 6, apartado 1, letra f), del RGPD de 2016, sobre licitud de la recogida y utilización de datos personales de los usuarios de sitios de medios en línea, quedaría menoscabado el principio si la normativa nacional excluye que el objetivo de garantizar el funcionamiento general del medio en línea pueda ocasionar un *juicio de ponderación* entre el interés legítimo del responsable del tratamiento y los derechos fundamentales de los usuarios objeto de protección.

Title:
Data protection at european livel in the sale of advertising spaces on the Internet: Combining information

Summary:

Resumen:

La jurisprudencia del Tribunal de Justicia de la Unión Europea ha ido profundizando en cómo la combinación de información fragmentaria sobre el usuario por operadores económicos diferentes, puede dar lugar a la composición de los datos personales del usuario, cuyo tratamiento es objeto de

protección por el Derecho de la Unión, particularmente en relación con la compra-venta de espacios publicitarios en Internet.

Abstract:

The case law of the Court of Justice of the European Union has been elaborating on how the combination of fragmentary information about the user by different economic operators can lead to the composition of the user's personal data, the processing of which is protected by EU law, particularly in relation to the purchase and sale of advertising space on the Internet.

Palabras clave:

Datos personales; combinación de datos.

Key words:

User's personal data; the combination of fragmentary information.