Sentencias del Tribunal de Justicia de la Unión Europea de 5 de junio y 10 de julio de 2018 (asuntos C-210/16 y C-25/17). Concepto de responsable del tratamiento

El Tribunal de Justicia de la Unión Europea (**TJUE**) ha publicado dos sentencias en las que, entre otras cuestiones, se profundiza sobre el concepto de responsable del tratamiento, tal y como lo define el artículo 2, letra d), de la Directiva 95/46/CE, esto es, como la persona física o jurídica que, sola *o conjuntamente con otros*, determina los fines y medios del tratamiento de los datos personales. El TJUE afirma que del tenor de este artículo no es posible inferir que el responsable haya de ser siempre, necesariamente, una sola persona. Por el contrario, es posible que varios agentes determinen los fines y medios de un tratamiento. De esta manera, el referido artículo da cabida a una responsabilidad conjunta respecto a un mismo tratamiento.

Sin embargo, precisa el TJUE, una responsabilidad conjunta no implica necesariamente una responsabilidad equivalente en la medida en la que la intervención de los agentes puede ser diversa, tanto en grado de intensidad como en las distintas etapas del tratamiento en que se produzca. Por tanto, su responsabilidad individual deberá evaluarse según las circunstancias del caso concreto. A esto añade que, para apreciar una responsabilidad conjunta, tampoco es necesario que cada uno de los agentes implicados tenga acceso a los datos personales en cuestión.

Por otra parte, en el asunto C-25/17, el TJUE se refiere a la interpretación del concepto de fichero. El supuesto analizado comprendía un conjunto de datos personales recogidos y tratados de forma manual por los miembros de una comunidad religiosa (Testigos de Jehová) con ocasión de una actividad de predicación puerta a puerta: nombres, direcciones e información relativa a personas contactadas. De conformidad con el Tribunal de Justicia, nos encontramos ante un fichero siempre que los datos estén estructurados según criterios determinados que permitan, en la práctica, recuperarlos fácilmente para su utilización posterior. En particular, para que un conjunto de datos que reúna estas características pueda ser concebido como un fichero, indica el Tribunal de Justicia que no es necesario que incluya fichas, catálogos específicos u otros sistemas de búsqueda. Tampoco importan la forma y criterios empleados para estructurarlo, sino únicamente que permita recuperar fácilmente los datos relativos a una determinada persona.

Finalmente, el TJUE aporta una serie de criterios para interpretar las excepciones al ámbito de aplicación de la citada Directiva. Respecto a la primera –tratamientos de datos que tengan por objeto la seguridad pública, la defensa y seguridad del Estado, etc.- aclara que se refiere siempre a actividades propias del Estado o de las autoridades estatales, ajenas por tanto a la esfera de los particulares.

La segunda contempla los tratamientos efectuados por una persona física en el ejercicio de actividades exclusivamente personales o domésticas. Éstas son las circunscritas al marco de la vida privada o familiar de los particulares, no pudiendo considerarse como tales aquéllas que tengan por objeto permitir a un número indeterminado de personas el acceso a los datos o que se extiendan, aun parcialmente, al espacio público.

Aquí pueden ser consultadas las sentencias C-210/16 y C-25/17.

Sentencia del Tribunal Constitucional 1405-2019, de 22 de mayo (rec. 1405/2019). Inconstitucionalidad del artículo 58 bis. 1 de la Ley del Régimen Electoral General

El Tribunal Constitucional (**TC**) ha publicado una sentencia en la que el Pleno, por unanimidad, declara la inconstitucionalidad y nulidad del apartado 1 del artículo 58 bis de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General (**LOREG**). El TC considera que esta disposición incurre en tres vulneraciones del artículo 18.4 –derecho fundamental a la protección de datos personales- en relación con el artículo 53.1 –principio de reserva de ley- de la Constitución Española (**CE**), infringiendo el mandato constitucional de preservación del contenido esencial del derecho fundamental.

La sentencia trae causa del recurso de inconstitucionalidad presentado el 5 de marzo de 2019 por el Defensor del Pueblo contra la citada disposición, que fue incorporada a la LOREG por la Disposición Final Tercera de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y autorizaba a los

partidos políticos a recoger datos personales relativos a las opiniones políticas de los ciudadanos con el siguiente tenor literal: *"La recopilación de datos personales relativos a las opiniones políticas de las personas que lleven a cabo los partidos políticos en el marco de sus actividades electorales se encontrará amparada en el interés público únicamente cuando se ofrezcan garantías adecuadas".*

El TC analiza tres elementos para valorar la constitucionalidad de la disposición impugnada:

(i) Si identifica la finalidad de la injerencia que supone en el derecho a la protección de los datos personales;

(ii) Si delimita los presupuestos y condiciones de tal injerencia; y

(iii) Si establece las garantías adecuadas para la protección del derecho afectado.

Respecto a la primera, afirma el TC que la legitimidad constitucional de la restricción del derecho fundamental a la protección de datos personales no puede estar basada en la invocación genérica de un indeterminado "interés público".

En cuanto a la segunda, el Tribunal pone de manifiesto que la disposición impugnada sólo contiene una condición limitativa del tratamiento, que únicamente podrá llevarse a cabo en el marco de las "actividades electorales" de los partidos políticos, condición que apenas delimita los presupuestos del tratamiento. De esta manera, la disposición carece de regla alguna sobre el alcance y contenido de los tratamientos que autoriza.

Finalmente, el TC entiende que el apartado 1 del artículo 58 bis de la LOREG no incorpora garantías adecuadas para proteger el derecho fundamental a la protección de datos personales. En este sentido, aclara que tales garantías deben estar incorporadas a la propia regulación legal del tratamiento, bien directamente o bien por remisión expresa y perfectamente delimitada a fuentes externas con rango normativo adecuado.

El texto íntegro de la sentencia puede ser consultado aquí.

Sentencia del Tribunal Supremo Nº 121/2019, de 5 de febrero (rec. 627/2018). Interpretación del concepto de establecimiento (artículo 2.1 a) LOPD 15/1999; artículo 3.1 a) RLOPD en relación con el artículo 4.1 a) de la Directiva 95/46/CE)

El Tribunal Supremo (**TS**) ha publicado una sentencia en la que interpreta el concepto de establecimiento previsto en el artículo 2.1 a) de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal (**LOPD**) y en el artículo 3.1 a) del Reglamento de desarrollo de la LOPD, en relación con el artículo 4.1 a) de la Directiva 95/46/CE y la jurisprudencia del Tribunal de Justicia de la Unión Europea que lo interpreta.

La sentencia trae causa del recurso de casación interpuesto por el Abogado del Estado, en nombre y representación de la Agencia Española de Protección de Datos (**AEPD**), frente a la sentencia de la Audiencia Nacional (**AN**) de 25 de octubre de 2017. En ella, la AN estima el recurso contencioso-administrativo presentado por TTI FINANCE, S.A.R.L. (**TTI**), entidad luxemburguesa, frente a una resolución sancionadora de la AEPD, al considerar que esa sociedad no tenía un establecimiento en España – que sólo poseía un apartado de correos y una cuenta bancaria en el país- y que, por tanto, la AEPD no podía exigirle el cumplimiento de la normativa española de protección de datos personales ni, en consecuencia, sancionarla por su infracción.

El TS admitió el recurso al entender que la interpretación del concepto de establecimiento, a fin de esclarecer si está sujeto a la normativa española de protección de datos un tratamiento realizado en nuestro país en el marco de las actividades de una empresa con sede en un tercer Estado Miembro y que cuenta para su desarrollo con cuenta bancaria y apartado de correos en España, presentaba interés casacional objetivo para la formación de jurisprudencia.

Tras realizar un recorrido por la normativa aplicable y la jurisprudencia que la interpreta, el TS pone de manifiesto que TTI no sólo contaba con un apartado de correos y una cuenta bancaria en España, sino que operaba a través de una sociedad con domicilio en Madrid que actuaba como apoderada y que disponía de dos personas de contacto que realizaban todas las gestiones necesarias para el desarrollo de la actividad de TTI.

Con base en todo ello, el TS estima el recurso y concluye que "*a los efectos de considerar si es aplicable la normativa de protección de datos de carácter personal de un Estado miembro de la Unión Europea a una empresa responsable del tratamiento de datos personales, en aquellos supuestos en que la sede principal esté ubicada en el territorio de otro Estado miembro de la Unión Europea, pero que realice actividades en otros Estados miembros, el concepto de establecimiento […] debe interpretarse de forma flexible y antiformalista, en el sentido de que resultan comprendidos el tratamiento de datos personales que se realiza en el marco o en el contexto de la actuación desarrollada en un Estado miembro de la Unión Europea (distinto a donde tiene la sede o administración principal) a través de la utilización de medios instrumentales que se revelen idóneos y eficaces en el tratamiento de datos personales*".

Sentencia completa disponible aquí.

Sentencia de la Audiencia Nacional de 23 de abril de 2019 (rec. 88/2017). Consideraciones sobre el empleo de un procedimiento sancionador como medio para sentar criterios generales por parte de la AEPD

La Audiencia Nacional (**AN**) ha publicado una sentencia cuyo interés radica no tanto en la cuestión de fondo sino en el reproche efectuado por el órgano judicial a la Agencia Española de Protección de Datos (**AEPD**).

Dicha sentencia resuelve el recurso contencioso-administrativo interpuesto por Google LLC (**Google**) frente a una resolución sancionadora de la AEPD, que le imponía una multa de 150.000 € por la comisión de una infracción tipificada como grave por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

La AN estima el recurso presentado por Google al entender que la AEPD no había respetado los principios rectores del procedimiento sancionador. En concreto, afirma este Tribunal que "*la AEPD, en este caso, no ha procedido a incoar un procedimiento sancionador, a partir de la denuncia de unos hechos concretos y en el que, respetando los principios que rigen tal procedimiento, haya llegado a una resolución sancionadora después de hacer una valoración razonable de las pruebas, sino que, como ella misma viene a reconocer, ha hecho uso de un procedimiento sancionador para establecer un criterio interpretativo respecto a las cuestiones planteadas por los denunciantes –el desacuerdo con los criterios ya establecidos por la propia AEPD en un comunicado de presa- conforme a las directrices del Grupo de Autoridades de protección de datos de la Unión Europea*".

Texto íntegro de la resolución aquí.

Lista de tratamientos de datos que requieren una evaluación de impacto relativa a protección de datos publicada por la Agencia Española de Protección de Datos

La Agencia Española de Protección de Datos (**AEPD**) ha publicado un listado orientativo y no exhaustivo de los tratamientos de datos personales para los que es obligatoria la realización de una evaluación de impacto relativa a la protección de datos (**EIPD**). La elaboración de esta lista responde a la previsión contenida en el apartado 4 del artículo 35 del Reglamento General de Protección de Datos (**RGPD**), de acuerdo a la que las autoridades de control establecerán y publicarán una lista de los tipos de operaciones de tratamiento que requieran una EIPD.

La EIPD se encuentra regulada en el art. 35 del RGPD. El apartado 1 impone a los responsables del tratamiento la obligación de realizar una de estas evaluaciones antes de dar inicio al tratamiento cuando sea probable que éste, a la vista de su naturaleza, alcance, contexto o fines, entrañe alto riesgo para los derechos y libertades de los interesados. Alto riesgo que se verá incrementado si el tratamiento, en palabras del RGPD, "*utiliza nuevas tecnologías*".

Por su parte, el apartado 3 del artículo contempla tres supuestos en los que es obligatoria la realización de una EIPD:

a) Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar.

b) Tratamiento a gran escala de categorías especiales de datos o de datos personales relativos a condenas e infracciones penales.

c) Observación sistemática a gran escala de una zona de acceso público.

La publicación de este listado tiene como objetivo complementar las disposiciones del RGPD y ofrecer seguridad jurídica a los responsables para identificar aquellos tratamientos en los que siempre se considerará probable la existencia de un alto riesgo. Además, los diferentes tipos de tratamientos incluidos en la lista no son excluyentes, sino complementarios. De esta manera, cuantas más características de las contempladas reúna el tratamiento en cuestión, mayor será la certeza de la necesidad de realizar una EIPD.

Acceso a la lista completa aquí.

FAQs relativas al tratamiento de datos en el ámbito laboral respondidas por AEPD

La Agencia Española de Protección de Datos (**AEPD**) ha incluido en su canal de consultas más frecuentes (**FAQs**) las respuestas a las preguntas recibidas en relación con el tratamiento de datos personales en el ámbito laboral.

Dicho canal tiene como finalidad proporcionar información sobre una gran variedad de cuestiones relacionadas con la protección de datos personales y vinculadas a las competencias de la AEPD: cuestiones generales del Reglamento General de Protección de Datos (**RGPD**), Delegados de Protección de Datos, derechos de los afectados, solvencia patrimonial o videovigilancia.

En este caso, se ha incorporado una categoría de FAQs denominada "13. Tratamiento de datos en el ámbito laboral", que se ocupa de diversos temas, incluido el control horario. En concreto –por ahora- la AEPD ha dado respuesta a cuestiones relativas a los datos que pueden incluir los justificantes de ausencias laborales y las tarjetas identificativas de los trabajadores, la posibilidad del comité de empresa de acceder al listado de trabajadores beneficiarios de la acción social, sistemas de fichaje basados en huella digital, comunicación de datos entre empresa subcontratada y principal, instalación de GPS en coches de empresa, solicitud de antecedentes penales para un puesto de trabajo, solicitud por el empresario de teléfono y correo electrónico particular del trabajador, comunicación de los resultados de reconocimientos médicos al empresario, comité de empresa y sección sindical y sistemas de control horario.

Todas las preguntas y respuestas de estos y otros temas aquí.

• • •

Si desea más información sobre estos temas o cualquier otro asunto relacionado, puede ponerse en contacto con el equipo de profesionales del área de Privacidad, IT y Entornos Digitales de BROSETA.

Área de Privacidad, IT y Entornos Digitales de BROSETA

Miguel Geijo
Socio. Director del Área
mgeijo@broseta.com

Agustín Puente
Socio
apuente@broseta.com

BROSETA

Madrid. Goya, 29. 28001. T. +34 914 323 144
Valencia. Pascual y Genís, 5. 46002. T. +34 963 921 006
Lisboa. Av. António Augusto Aguiar, 15. 1050-012. T. +351 300 509 035
Zúrich. Schützengasse 4, 8001. T. +41 44 520 81 03

Firma miembro de la **Red Legal Iberoamericana**